This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problems Mailbox.

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION CONCERNING
AMENDMENTS OF THE CLAIMS

(PCT Rule 62 and
Administrative Instructions, Section 417)

To:

Commissioner
US Department of Commerce
United States Patent and Trademark
Office, PCT
2011 South Clark Place Room
CP2/5C24
Arlington, VA 22202
ETATS-UNIS D'AMERIQUE

in its capacity as International Preliminary Examining Authority

Date of mailing (day/month/year)	
24 August 2001 (24.08.01)	
International application No.	International filing date (day/month/year)
PCT/IL00/00555	10 September 2000 (10.09.00)

Applicant

M-SYSTEMS FLASH DISK PIONEERS LTD. et al

The International Bureau hereby informs the International Preliminary Examining Authority that no amendments under Article 19 have been received by the International Bureau (Administrative Instructions, Section 417).

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No. (41-22) 740.14.35

Authorized officer

ALi SOLEIMAN

Telephone No. (41-22) 338.83.38

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF THE RECORDING OF A CHANGE

(PCT Rule 92bis.1 and Administrative Instructions, Section 422)

To:

BRASS, Daniel
Beit Agish Ravad
Noach Mozes Street 13
67442 Tel Aviv
ISRAËL

Date of mailing (day/month/year)
07 November 2000 (07.11.00)

Applicant's or agent's file reference
M01/3

IMPORTANT NOTIFICATION

International application No.
PCT/IL00/00555

International filing date (day/month/year)
10 September 2000 (10.09.00)

1. The following indications appeared on record concerning:

[X] the applicant [ ] the inventor [ ] the agent [ ] the common representative

Name and Address

State of Nationality | State of Residence

Telephone No.

Facsimile No.

Teleprinter No.

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

[X] the person [X] the name [X] the address [ ] the nationality [ ] the residence

Name and Address

RAZ, Dan
30 Borohov Street
Apt. No. 6
64252 Tel Aviv
Israel

State of Nationality: IL | State of Residence: IL

Telephone No.

Facsimile No.

Teleprinter No.

3. Further observations, if necessary:

Additional applicant and inventor for US only.

4. A copy of this notification has been sent to:

[X] the receiving Office
[X] the International Searching Authority
[ ] the International Preliminary Examining Authority
[ ] the designated Offices concerned
[ ] the elected Offices concerned
[ ] other:

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer

C. Cupello

Telephone No.: (41-22) 338.83.38

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION RELATING TO PRIORITY CLAIM

(PCT Rules 26bis.1 and 26bis.2 and Administrative Instructions, Sections 402 and 409)

To:

BRASS, Daniel
Plinner, Bodner & Brass
Beit Agish Ravad
13 Noach Mozes Street
67442 Tel Aviv
ISRAËL

Date of mailing (day/month/year) 13 December 2000 (13.12.00)	
Applicant's or agent's file reference M01/3	**IMPORTANT NOTIFICATION**
International application No. PCT/IL00/00555	International filing date (day/month/year) 10 September 2000 (10.09.00)
Applicant M-SYSTEMS FLASH DISK PIONEERS LTD. et al	

The applicant is hereby **notified** of the following in respect of the priority claim(s) made in the international application.

1. [X] **Correction of priority claim.** In accordance with the applicant's notice received on: 22 November 2000 (22.11.00), the following priority claim has been corrected to read as follows:

US 17 April 2000 (17.04.00) 09/550,491

- [ ] even though the indication of the number of the earlier application is missing.
- [ ] even though the following indication in the priority claim is not the same as the corresponding indication appearing in the priority document:

2. [ ] **Addition of priority claim.** In accordance with the applicant's notice received on: , the following priority claim has been added:

- [ ] even though the indication of the number of the earlier application is missing.
- [ ] even though the following indication in the priority claim is not the same as the corresponding indication appearing in the priority document:

3. [ ] As a **result of the correction and/or addition** of (a) priority claim(s) under items 1 and/or 2, the (earliest) priority date is:

4. [ ] **Priority claim considered not to have been made.**

- [ ] The applicant failed to respond to the Invitation under Rule 26bis.2(a) (Form PCT/IB/316) within the prescribed time limit.
- [ ] The applicant's notice was received after the expiration of the prescribed time limit under Rule 26bis.1(a).
- [ ] The applicant's notice failed to correct the priority claim so as to comply with the requirements of Rule 4.10.

The applicant may, before the technical preparations for international publication have been completed and subject to the payment of a fee, request the International Bureau to publish, together with the international application, information concerning the priority claim. See Rule 26bis.2(c) and the PCT Applicant's Guide, Volume I, Annex B2(IB).

5. [ ] In case where **multiple priorities** have been claimed, the above item(s) relate to the following priority claim(s):

6. A copy of this notification has been sent to the receiving Office and

- [X] to the International Searching Authority (where the international search report has not yet been issued).
- [X] the designated Offices (which have already been notified of the receipt of the record copy).

The International Bureau of WIPO **34, chemin des Colombettes** **1211 Geneva 20, Switzerland**	Authorized officer Céline Faust
Facsimile No. (41-22) 740.14.35	Telephone No. (41-22) 338.83.38

Form PCT/IB/318 (July 1998)

003719838

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION RELATING TO PRIORITY CLAIM

(PCT Rules 26bis.1 and 26bis.2 and Administrative Instructions, Sections 402 and 409)

To:

BRASS, Daniel
Plinner, Bodner & Brass
Beit Agish Ravad
13 Noach Mozes Street
67442 Tel Aviv
ISRAËL

Date of mailing (day/month/year) 13 December 2000 (13.12.00)	
Applicant's or agent's file reference M01/3	**IMPORTANT NOTIFICATION**
International application No. PCT/IL00/00555	International filing date (day/month/year) 10 September 2000 (10.09.00)
Applicant M-SYSTEMS FLASH DISK PIONEERS LTD. et al	

The applicant is hereby **notified** of the following in respect of the priority claim(s) made in the international application.

1. [X] **Correction of priority claim.** In accordance with the applicant's notice received on: 22 November 2000 (22.11.00), the following priority claim has been corrected to read as follows:

   US 17 April 2000 (17.04.00) 09/550,491

   [ ] even though the indication of the number of the earlier application is missing.
   [ ] even though the following indication in the priority claim is not the same as the corresponding indication appearing in the priority document:

2. [ ] **Addition of priority claim.** In accordance with the applicant's notice received on: , the following priority claim has been added:

   [ ] even though the indication of the number of the earlier application is missing.
   [ ] even though the following indication in the priority claim is not the same as the corresponding indication appearing in the priority document:

3. [ ] As a **result of the correction and/or addition** of (a) priority claim(s) under items 1 and/or 2, the (earliest) priority date is:

4. [ ] **Priority claim considered not to have been made.**
   [ ] The applicant failed to respond to the Invitation under Rule 26bis.2(a) (Form PCT/IB/316) within the prescribed time limit.
   [ ] The applicant's notice was received after the expiration of the prescribed time limit under Rule 26bis.1(a).
   [ ] The applicant's notice failed to correct the priority claim so as to comply with the requirements of Rule 4.10.

   The applicant may, before the technical preparations for international publication have been completed and subject to the payment of a fee, request the International Bureau to publish, together with the international application, information concerning the priority claim. See Rule 26bis.2(c) and the PCT Applicant's Guide, Volume I, Annex B2(IB).

5. [ ] In case where **multiple priorities** have been claimed, the above item(s) relate to the following priority claim(s):

6. A copy of this notification has been sent to the receiving Office and
   [X] to the International Searching Authority (where the international search report has not yet been issued).
   [X] the designated Offices (which have already been notified of the receipt of the record copy).

The International Bureau of WIPO **34, chemin des Colombettes** **1211 Geneva 20, Switzerland**	Authorized officer Céline Faust
Facsimile No. (41-22) 740.14.35	Telephone No. (41-22) 338.83.38

Form PCT/IB/318 (July 1998)

003719838

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF THE RECORDING OF A CHANGE

(PCT Rule 92bis.1 and Administrative Instructions, Section 422)

To:

BRASS, Daniel
Plinner, Bodner & Brass
Beit Agish Ravad
13 Noach Mozes Street
67442 Tel Aviv
ISRAËL

Date of mailing (day/month/year)
13 December 2000 (13.12.00)

Applicant's or agent's file reference
M01/3

IMPORTANT NOTIFICATION

International application No.
PCT/IL00/00555

International filing date (day/month/year)
10 September 2000 (10.09.00)

1. The following indications appeared on record concerning:

☐ the applicant ☐ the inventor ☒ the agent ☐ the common representative

Name and Address

BRASS, Daniel
Beit Agish Ravad
Noach Mozes Street 13
67442 Tel Aviv
Israel

State of Nationality:
State of Residence:
Telephone No.: 972-3-696-9090
Facsimile No.: 972-3-696-6656
Teleprinter No.:

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

☐ the person ☐ the name ☒ the address ☐ the nationality ☐ the residence

Name and Address

BRASS, Daniel
Plinner, Bodner & Brass
Beit Agish Ravad
13 Noach Mozes Street
67442 Tel Aviv
Israel

State of Nationality:
State of Residence:
Telephone No.: 972-3-696-9090
Facsimile No.: 972-3-696-6656
Teleprinter No.:

3. Further observations, if necessary:

4. A copy of this notification has been sent to:

☒ the receiving Office
☒ the International Searching Authority
☐ the International Preliminary Examining Authority
☐ the designated Offices concerned
☐ the elected Offices concerned
☐ other:

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer
Céline Faust

Telephone No.: (41-22) 338.83.38

Form PCT/IB/306 (March 1994)

003719779

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF THE RECORDING OF A CHANGE

(PCT Rule 92bis.1 and Administrative Instructions, Section 422)

To:

BRASS, Daniel
Plinner, Bodner & Brass
Beit Agish Ravad
13 Noach Mozes Street
67442 Tel Aviv
ISRAËL

Date of mailing (day/month/year)
13 December 2000 (13.12.00)

Applicant's or agent's file reference
M01/3

IMPORTANT NOTIFICATION

International application No.
PCT/IL00/00555

International filing date (day/month/year)
10 September 2000 (10.09.00)

1. The following indications appeared on record concerning:

[X] the applicant [X] the inventor [ ] the agent [ ] the common representative

Name and Address
RAZ, Dan
30 Borohov Street
Apt. No. 6
64252 Tel Aviv
Israel

State of Nationality: IL
State of Residence: IL
Telephone No.:
Facsimile No.:
Teleprinter No.:

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

[ ] the person [X] the name [ ] the address [ ] the nationality [ ] the residence

Name and Address
DAN, Raz
30 Borohov Street
Apt. No. 6
64252 Tel Aviv
Israel
Israel

State of Nationality: IL
State of Residence: IL
Telephone No.:
Facsimile No.:
Teleprinter No.:

3. Further observations, if necessary:

4. A copy of this notification has been sent to:

[X] the receiving Office
[X] the International Searching Authority
[ ] the International Preliminary Examining Authority
[ ] the designated Offices concerned
[ ] the elected Offices concerned
[ ] other:

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer
Céline Faust

Telephone No.: (41-22) 338.83.38

Form PCT/IB/306 (March 1994)

003719781

PATENT COOPERATION TREATY

REC'D 19 SEP 2001
WIPO PCT

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

14

Applicant's or agent's file reference MO1/3	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/IL00/00555	International filing date *(day/month/year)* 10 SEPTEMBER 2000	Priority date *(day/month/year)* 30 SEPTEMBER 1999
International Patent Classification (IPC) or national classification and IPC Please See Supplemental Sheet.		
Applicant M-SYSTEMS FLASH DISK PIONEERS LTD.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets.

   ☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority. (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 6 sheets.

3. This report contains indications relating to the following items:

   I ☒ Basis of the report

   II ☐ Priority

   III ☐ Non-establishment of report with regard to novelty, inventive step or industrial applicability

   IV ☐ Lack of unity of invention

   V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

   VI ☒ Certain documents cited

   VII ☐ Certain defects in the international application

   VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
18 APRIL 2001	05 AUGUST 2001
Name and mailing address of the IPEA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer Peggy Harwood PAUL R. LINTZ PH.D. Telephone No. (703) 305-3832

Form PCT/IPEA/409 (cover sheet) (July 1998) ★

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

Internat[redacted]application No.
PCT/IL00/00555

I. Basis f the report

1. With regard to the **elements** of the international application:*

[X] the international application as originally filed

[X] the description:
pages 1-21 , as originally filed
pages NONE , filed with the demand
pages NONE , filed with the letter of _____

[X] the claims:
pages 22-31 , as originally filed
pages NONE , as amended (together with any statement) under Article 19
pages NONE , filed with the demand
pages NONE , filed with the letter of _____

[X] the drawings:
pages 1-6 , as originally filed
pages NONE , filed with the demand
pages NONE , filed with the letter of _____

[X] the sequence listing part of the description:
pages NONE , as originally filed
pages NONE , filed with the demand
pages NONE , filed with the letter of _____

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language _____ which is:

[ ] the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).

[ ] the language of publication of the international application (under Rule 48.3(b)).

[ ] the language of the translation furnished for the purposes of international preliminary examination (under Rules 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

[ ] contained in the international application in printed form.

[ ] filed together with the international application in computer readable form.

[ ] furnished subsequently to this Authority in written form.

[ ] furnished subsequently to this Authority in computer readable form.

[ ] The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

[ ] The statement that the information recorded in computer readable form is identical to the writen sequence listing has been furnished.

4. [X] The amendments have resulted in the cancellation of:

[X] the description, pages NONE

[X] the claims, Nos. NONE

[X] the drawings, sheets/~~fig~~ NONE

5. [ ] This report has been drawn as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

** Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17).*

***Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.*

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

Internati[redacted]application No.
PCT/IL00/00555

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step r industrial applicability; citations and explanations supporting such statement

1. statement

Novelty (N)	Claims	1-50	YES
	Claims	NONE	NO
Inventive Step (IS)	Claims	1-50	YES
	Claims	NONE	NO
Industrial Applicability (IA)	Claims	1-50	YES
	Claims	NONE	NO

2. citations and explanations (Rule 70.7)

Claims 1-50 meet the criteria set out in PCT Article 33(2)-(4), because the prior art does not teach or fairly suggest all the limitations of the independent claims taken together. The closest prior art were P and T references.

---------- NEW CITATIONS ----------

US 6,040,622 A (WALLACE) 21 March 2000, see Abstract,Column 1, lines 10-21.

US 6,147,860 A (IWASAKI) 14 November 2000, See Column 6, lines 20-23; lines 55-57.

US 6,240,493 B1 (HARDWOOD, III et al.),29 MAY 2001 See Figure 1, Figure 2.

VI. Certain documents cited

1. Certain published documents (Rule 70.10)

Application No. Patent No.	Publication Date *(day/month/year)*	Filing Date *(day/month/year)*	Priority date (valid claim) *(day/month/year)*
US, B1, 6,240,493	29 MAY 2001	17 APRIL 1999	17 APRIL 1999
US, A, 6,147,860	14 NOVEMBER 2000	14 MARCH 1997	4 MARCH 1994
US, A, 6,040,622	21 MARCH 2000	11 JUNE 1998	11 JUNE 1998

2. Non-written disclosures (Rule 70.9)

Kind of non-written disclosure	Date of non-written disclosure *(day/month/year)*	Date of written disclosure referring to non-written disclosure *(day/month/year)*

Supplemental Box
(To be used when the space in any of the preceding boxes is not sufficient)

Continuation of: Boxes I - VIII

CLASSIFICATION:

The International Patent Classification (IPC) and/or the National classification are as listed below:

IPC(7): G06F 1/24,11/30,17/30,17/60;G08B 19/02;H01L 23/02, and US Cl.:
707/8;705/41;713/186;340/5.81,5.82;235/379,382;257/679

PCT

REQUEST

The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty.

For receiving Office use only

International Application [redacted]

International Filing Date

Name of receiving Office and "PCT International Application"

Applicant's or agent's file reference *(if desired) (12 characters maximum)* M01/3

Box No. I TITLE OF INVENTION

REMOVABLE, ACTIVE, PERSONAL STORAGE DEVICE, SYSTEM AND METHOD

Box No. II APPLICANT

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

M-SYSTEMS FLASH DISK PIONEERS LTD.
KIRYAT ATIDIM
P.O. BOX 58036
TEL AVIV 61580
ISRAEL

☐ This person is also inventor.

Telephone No.
972-3-647-7776

Facsimile No.
972-3-647-6668

Teleprinter No.

State *(that is, country)* of nationality:
ISRAEL

State *(that is, country)* of residence:
ISRAEL

This person is applicant for the purposes of: ☐ all designated States ☒ all designated States except the United States of America ☐ the United States of America only ☐ the States indicated in the Supplemental Box

Box No. III FURTHER APPLICANT(S) AND/OR (FURTHER) INVENTOR(S)

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

MORAN, DOV
15 ITAMAR-BEN-AVI
KFAR SABA
44406
ISRAEL

This person is:

☐ applicant only

☒ applicant and inventor

☐ inventor only *(If this check-box is marked, do not fill in below.)*

State *(that is, country)* of nationality:
ISRAEL

State *(that is, country)* of residence:
ISRAEL

This person is applicant for the purposes of: ☐ all designated States ☐ all designated States except the United States of America ☒ the United States of America only ☐ the States indicated in the Supplemental Box

☒ Further applicants and/or (further) inventors are indicated on a continuation sheet.

Box No. IV AGENT OR COMMON REPRESENTATIVE; OR ADDRESS FOR CORRESPONDENCE

The person identified below is hereby/has been appointed to act on behalf of the applicant(s) before the competent International Authorities as: ☒ agent ☐ common representative

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

BRASS, DANIEL
Beit Agish Ravad
13 Noach Mozes Street
Tel Aviv 67442
ISRAEL

Telephone No.
972-3-696-9090

Facsimile No.
972-3-696-6656

Teleprinter No.

☐ **Address for correspondence:** Mark this check-box where no agent or common representative is/has been appointed and the space above is used instead to indicate a special address to which correspondence should be sent.

Continuati n of Box No. III FU[redacted]HER APPLICANTS AND/OR (FURTHE[redacted]VENTOR(S)

If none of the following sub-boxes is used, this sheet is not to be included in the request.

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*
ELAZAR, GIDI

This person is:
- ☐ applicant only
- ☒ applicant and inventor
- ☐ inventor only *(If this check-box is marked, do not fill in below.)*

State *(that is, country)* of nationality: ISRAEL

State *(that is, country)* of residence: ISRAEL

This person is applicant for the purposes of: ☐ all designated States ☐ all designated States except the United States of America ☒ the United States of America only ☐ the States indicated in the Supplemental Box

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*
HARKABI, DAN

This person is:
- ☐ applicant only
- ☒ applicant and inventor
- ☐ inventor only *(If this check-box is marked, do not fill in below.)*

State *(that is, country)* of nationality: ISRAEL

State *(that is, country)* of residence: ISRAEL

This person is applicant for the purposes of: ☐ all designated States ☐ all designated States except the United States of America ☒ the United States of America only ☐ the States indicated in the Supplemental Box

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

This person is:
- ☐ applicant only
- ☐ applicant and inventor
- ☐ inventor only *(If this check-box is marked, do not fill in below.)*

State *(that is, country)* of nationality:

State *(that is, country)* of residence:

This person is applicant for the purposes of: ☐ all designated States ☐ all designated States except the United States of America ☐ the United States of America only ☐ the States indicated in the Supplemental Box

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

This person is:
- ☐ applicant only
- ☐ applicant and inventor
- ☐ inventor only *(If this check-box is marked, do not fill in below.)*

State *(that is, country)* of nationality:

State *(that is, country)* of residence:

This person is applicant for the purposes of: ☐ all designated States ☐ all designated States except the United States of America ☐ the United States of America only ☐ the States indicated in the Supplemental Box

☐ Further applicants and/or (further) inventors are indicated on another continuation sheet.

Box No.V DESIGNATION OF STATES

The following designations are hereby m[redacted]der Rule 4.9(a) *(mark the applicable check-boxe[redacted]ast one must be marked):*

Regional Patent

☒ **AP ARIPO Patent:** **GH** Ghana, **GM** Gambia, **KE** Kenya, **LS** Lesotho, **MW** Malawi, **SD** Sudan, **SL** Sierra Leone, **SZ** Swaziland, **TZ** United Republic of Tanzania, **UG** Uganda, **ZW** Zimbabwe, and any other State which is a Contracting State of the Harare Protocol and of the PCT

☒ **EA Eurasian Patent:** **AM** Armenia, **AZ** Azerbaijan, **BY** Belarus, **KG** Kyrgyzstan, **KZ** Kazakhstan, **MD** Republic of Moldova, **RU** Russian Federation, **TJ** Tajikistan, **TM** Turkmenistan, and any other State which is a Contracting State of the Eurasian

☒ **EP European Patent:** **AT** Austria, **BE** Belgium, **CH and LI** Switzerland and Liechtenstein, **CY** Cyprus, **DE** Germany, **DK** Denmark, **ES** Spain, **FI** Finland, **FR** France, **GB** United Kingdom, **GR** Greece, **IE** Ireland, **IT** Italy, **LU** Luxembourg, **MC** Monaco, **NL** Netherlands, **PT** Portugal, **SE** Sweden, and any other State which is a Contracting State of the European Patent Convention and of the PCT

☒ **OA OAPI Patent:** **BF** Burkina Faso, **BJ** Benin, **CF** Central African Republic, **CG** Congo, **CI** Côte d'Ivoire, **CM** Cameroon, **GA** Gabon, **GN** Guinea, **GW** Guinea-Bissau, **ML** Mali, **MR** Mauritania, **NE** Niger, **SN** Senegal, **TD** Chad, **TG** Togo, and any other State which is a member State of OAPI and a Contracting State of the PCT *(if other kind of protection or treatment desired, specify on dotted line)* . . . . . .

National Patent *(if other kind of protection or treatment desired, specify on dotted line):*

☒ **AE** United Arab Emirates
☒ **AL** Albania . . . . . .
☒ **AM** Armenia . . . . . .
☒ **AT** Austria . . . . . .
☒ **AU** Australia . . . . . .
☒ **AZ** Azerbaijan
☒ **BA** Bosnia and Herzegovina . . . . . .
☒ **BB** Barbados
☒ **BG** Bulgaria . . . . . .
☒ **BR** Brazil . . . . . .
☒ **BY** Belarus . . . . . .
☒ **CA** Canada
☒ **CH and LI** Switzerland and Liechtenstein
☒ **CN** China . . . . . .
☒ **CR** Costa Rica . . . . . .
☒ **CU** Cuba . . . . . .
☒ **CZ** Czech Republic . . . . . .
☒ **DE** Germany . . . . . .
☒ **DK** Denmark . . . . . .
☒ **DM** Dominica
☒ **EE** Estonia . . . . . .
☒ **ES** Spain . . . . . .
☒ **FI** Finland . . . . . .
☒ **GB** United Kingdom
☒ **GD** Grenada
☒ **GE** Georgia . . . . . .
☒ **GH** Ghana . . . . . .
☒ **GM** Gambia
☒ **HR** Croatia . . . . . .
☒ **HU** Hungary . . . . . .
☒ **ID** Indonesia
☒ **IL** Israel . . . . . .
☒ **IN** India . . . . . .
☒ **IS** Iceland
☒ **JP** Japan . . . . . .
☒ **KE** Kenya . . . . . .
☒ **KG** Kyrgyzstan . . . . . .
☒ **KP** Democratic People's Republic of Korea . . . . . .
☒ **KR** Republic of Korea . . . . . .
☒ **KZ** Kazakhstan . . . . . .
☒ **LC** Saint Lucia
☒ **LK** Sri Lanka
☒ **LR** Liberia
☒ **LS** Lesotho . . . . . .
☒ **LT** Lithuania
☒ **LU** Luxembourg
☒ **LV** Latvia
☒ **MA** Morocco . . . . . .
☒ **MD** Republic of Moldova . . . . . .
☒ **MG** Madagascar . . . . . .
☒ **MK** The former Yugoslav Republic of Macedonia . . . . . .
☒ **MN** Mongolia
☒ **MW** Malawi . . . . . .
☒ **MX** Mexico . . . . . .
☒ **NO** Norway
☒ **NZ** New Zealand . . . . . .
☒ **PL** Poland . . . . . .
☒ **PT** Portugal . . . . . .
☒ **RO** Romania
☒ **RU** Russian Federation . . . . . .
☒ **SD** Sudan
☒ **SE** Sweden
☒ **SG** Singapore
☒ **SI** Slovenia . . . . . .
☒ **SK** Slovakia . . . . . .
☒ **SL** Sierra Leone . . . . . .
☒ **TJ** Tajikistan . . . . . .
☒ **TM** Turkmenistan . . . . . .
☒ **TR** Turkey . . . . . .
☒ **TT** Trinidad and Tobago . . . . . .
☒ **TZ** United Republic of Tanzania
☒ **UA** Ukraine . . . . . .
☒ **UG** Uganda . . . . . .
☒ **US** United States of America . . . . . .
☒ **UZ** Uzbekistan . . . . . .
☒ **VN** Viet Nam . . . . . .
☒ **YU** Yugoslavia . . . . . .
☒ **ZA** South Africa . . . . . .
☒ **ZW** Zimbabwe . . . . . .

Check-boxes reserved for designating States which have become party to the PCT after issuance of this sheet:

☐ . . . . . .
☐ . . . . . .

Precautionary Designation Statement: In addition to the designations made above, the applicant also makes under Rule 4.9(b) all other designations which would be permitted under the PCT except any designation(s) indicated in the Supplemental Box as being excluded from the scope of this statement. The applicant declares that those additional designations are subject to confirmation and that any designation which is not confirmed before the expiration of 15 months from the priority date is to be regarded as withdrawn by the applicant at the expiration of that time limit. *(Confirmation (including fees) must reach the receiving Office within the 15-month time limit.)*

Box No. VI PRIORITY CLAIM ☐ Further priority claims are indicated in the Supplemental Box.

Filing date of earlier application (day/month/year)	Number of earlier application	Where earlier application is: national application: country	regional application:* regional Office	international application: receiving Office
item (1) 30 SEPT 1999 (30/09/99)	09/409,091	US		
item (2) 17 MAR 2000 (17/04/99)	09/550,491	US		
item (3)				

☐ The receiving Office is requested to prepare and transmit to the International Bureau a certified copy of the earlier application(s) *(only if the earlier application was filed with the Office which for the purposes of the present international application is the receiving Office)* identified above as item(s): _____

* *Where the earlier application is an ARIPO application, it is mandatory to indicate in the Supplemental Box at least one country party to the Paris Convention for the Protection of Industrial Property for which that earlier application was filed (Rule 4.10(b)(ii)). See Supplemental Box.*

Box No. VII INTERNATIONAL SEARCHING AUTHORITY

Choice of International Searching Authority (ISA) *(if two or more International Searching Authorities are competent to carry out the international search, indicate the Authority chosen; the two-letter code may be used):*

ISA/ US

Request to use results of earlier search; reference to that search *(if an earlier search has been carried out by or requested from the International Searching Authority):*

Date *(day/month/year)* Number Country (or regional Office)

Box No. VIII CHECK LIST: LANGUAGE OF FILING

This international application contains the following **number of sheets:**

request	:	4
description (excluding sequence listing part)	:	21
claims	:	10
abstract	:	1
drawings	:	6
sequence listing part of description	:	
Total number of sheets	:	42

This international application is **accompanied** by the item(s) marked below:

1. ☒ fee calculation sheet
2. ☐ separate signed power of attorney
3. ☐ copy of general power of attorney; reference number, if any:
4. ☐ statement explaining lack of signature
5. ☐ priority document(s) identified in Box No. VI as item(s):
6. ☐ translation of international application into (language):
7. ☐ separate indications concerning deposited microorganism or other biological material
8. ☐ nucleotide and/or amino acid sequence listing in computer readable form
9. ☐ other *(specify)*:

Figure of the drawings which should accompany the abstract: 1

Language of filing of the international application: ENGLISH

Box No. IX SIGNATURE OF APPLICANT OR AGENT

Next to each signature, indicate the name of the person signing and the capacity in which the person signs (if such capacity is not obvious from reading the request).

DANIEL BRASS

For receiving Office use only

1. Date of actual receipt of the purported international application:	2. Drawings: ☐ received: ☐ not received:
3. Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application:	
4. Date of timely receipt of the required corrections under PCT Article 11(2):	
5. International Searching Authority (if two or more are competent): ISA/	6. ☐ Transmittal of search copy delayed until search fee is paid.

For International Bureau use only

Date of receipt of the record copy by the International Bureau:

This sheet is not part of and does not count as a sheet of the international application.

PCT

FEE CALCULATION SHEET

Annex to the Request

For receiving Office use only

International application No.

Date stamp of the receiving Office

Applicant's or agent's file reference: **M01/3**

Applicant: **M-SYSTEMS FLASH DISK PIONEERS LTD.**

CALCULATION OF PRESCRIBED FEES

1. TRANSMITTAL FEE . . . . . NIS 437.00 T

2. SEARCH FEE . . . . . 700.00 S

International search to be carried out by **US**

(If two or more International Searching Authorities are competent in relation to the international application, indicate the name of the Authority which is chosen to carry out the international search.)

3. INTERNATIONAL FEE

Basic Fee

The international application contains **42** sheets.

first 30 sheets 427.00 b1

12 remaining sheets x **$10.00** additional amount = 120.00 b2

Add amounts entered at b1 and b2 and enter total at B . . 547.00 B

Designation Fees

The international application contains **ALL** designations.

8 number of designation fees payable *(maximum 8)* x **92.00** amount of designation fee = 736.00 D

Add amounts entered at B and D and enter total at I . . . . . 1,283.00 I

(Applicants from certain States are entitled to a reduction of 75% of the international fee. Where the applicant is (or all applicants are) so entitled, the

4. FEE FOR PRIORITY DOCUMENT *(if applicable)* . . . . . P

5. TOTAL FEES PAYABLE . . . . . 437 / NIS $1,983.00 TOTAL

Add amounts entered at T, S, I and P, and enter total in the TOTAL box

☒ The designation fees are not paid at this time.

MODE OF PAYMENT

- ☐ authorization to charge deposit account (see below)
- ☐ bank draft
- ☐ coupons
- ☐ cheque
- ☐ cash
- ☐ other *(specify)*:
- ☒ postal money order
- ☐ revenue stamps

DEPOSIT ACCOUNT AUTHORIZATION *(this mode of payment may not be available at all receiving Offices)*

The RO/ _____

- ☐ is hereby authorized to charge the total fees indicated above to my deposit account.
- ☐ *(this check-box may be marked only if the conditions for deposit accounts of the receiving Office so permit)* is hereby authorized to charge any deficiency or credit any overpayment in the total fees indicated above to my deposit account.
- ☐ is hereby authorized to charge the fee for preparation and transmittal of the priority document to the International Bureau of WIPO to my deposit account.

Deposit Account No. | Date *(day/month/year)* | Signature

PATENT COOPERATION TREATY

From the
INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

To: DANIEL BRASS
BEIT AGISH RAVAD
13 NOACH MOZES STREET
TEL AVIV 67442
ISRAEL

PCT

NOTIFICATION OF TRANSMITTAL OF INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Rule 71.1)

Date of Mailing *(day/month/year)*	14 SEP 2001
Applicant's or agent's file reference: MO1/3	**IMPORTANT NOTIFICATION**

International application No.	International filing date *(day/month/year)*	Priority Date *(day/month/year)*
PCT/IL00/00555	10 SEPTEMBER 2000	30 SEPTEMBER 1999

Applicant: M-SYSTEMS FLASH DISK PIONEERS LTD.

1. The applicant is hereby notified that this International Preliminary Examining Authority transmits herewith the international preliminary examination report and its annexes, if any, established on the international application.

2. A copy of the report and its annexes, if any, is being transmitted to the International Bureau for communication to all the elected Offices.

3. Where required by any of the elected Offices, the International Bureau will prepare an English translation of the report (but not of any annexes) and will transmit such translation to those Offices.

4. REMINDER

The applicant must enter the national phase before each elected Office by performing certain acts (filing translations and paying national fees) within 30 months from the priority date (or later in some Offices)(Article 39(1))(see also the reminder sent by the International Bureau with Form PCT/IB/301).

Where a translation of the international application must be furnished to an elected Office, that translation must contain a translation of any annexes to the international preliminary examination report. It is the applicant's responsibility to prepare and furnish such translation directly to each elected Office concerned.

For further details on the applicable time limits and requirements of the elected Offices, see Volume II of the PCT Applicant's Guide.

Name and mailing address of the IPEA/US	Authorized officer
Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231	PAUL R. LINTZ PH.D. Peggy Harrod
Facsimile No. (703) 305-3230	Telephone No. (703) 305-3832

Form PCT/IPEA/416 (July 1992)★

פלינר, כוכר, ברס
19 -11- 2000
PCT

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

To:
BRASS, Daniel
Beit Agish Ravad
Noach Mozes Street 13
67442 Tel Aviv
ISRAEL

COMMUNICATION IN CASES FOR WHICH NO OTHER FORM IS APPLICABLE

Date of mailing (*day/month/year*) 07 November 2000 (07.11.00)	
Applicant's or agent's file reference M01/3	**REPLY DUE** see paragraph 1 below
International application No. PCT/IL00/00555	International filing date (*day/month/year*) 10 September 2000 (10.09.00)
Applicant M-SYSTEMS FLASH DISK PIONEERS LTD.	

1. ☐ REPLY DUE within _____ months/days from the above date of mailing

☐ NO REPLY DUE, however, see below

☒ IMPORTANT COMMUNICATION

☐ INFORMATION ONLY

2. COMMUNICATION:

The International Bureau received on 16 October 2000 (16.10.00) a 92bis request for the above-mentioned international application. Please be informed that a power of attorney for the new applicant and inventor RAZ, Dan is requested authorizing you to represent him.

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland	Authorized officer C. Cupello
Facsimile No. (41-22) 740.14.35	Telephone No. (41-22) 338.83.38

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF THE RECORDING OF A CHANGE

(PCT Rule 92bis.1 and Administrative Instructions, Section 422)

To:

BRASS, Daniel
Beit Agish Ravad
Noach Mozes Street 13
67442 Tel Aviv
ISRAËL

Date of mailing (day/month/year)
07 November 2000 (07.11.00)

Applicant's or agent's file reference
M01/3

IMPORTANT NOTIFICATION

International application No.
PCT/IL00/00555

International filing date (day/month/year)
10 September 2000 (10.09.00)

1. The following indications appeared on record concerning:

[X] the applicant [ ] the inventor [ ] the agent [ ] the common representative

Name and Address

State of Nationality

State of Residence

Telephone No.

Facsimile No.

Teleprinter No.

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

[X] the person [X] the name [X] the address [ ] the nationality [ ] the residence

Name and Address

RAZ, Dan
30 Borohov Street
Apt. No. 6
64252 Tel Aviv
Israel

State of Nationality: IL

State of Residence: IL

Telephone No.

Facsimile No.

Teleprinter No.

3. Further observations, if necessary:

Additional applicant and inventor for US only.

4. A copy of this notification has been sent to:

[X] the receiving Office
[X] the International Searching Authority
[ ] the International Preliminary Examining Authority
[ ] the designated Offices concerned
[ ] the elected Offices concerned
[ ] other:

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer

C. Cupello

Telephone No.: (41-22) 338.83.38

פלינר, בדנר, ברס
06 -11- 2000
נתקבל

PATENT COOPERATION TREATY

PCT

From the INTERNATIONAL BUREAU

To:

BRASS, Daniel
Beit Agish Ravad
Noach Mozes Street 13
67442 Tel Aviv
ISRAËL

NOTIFICATION OF RECEIPT OF RECORD COPY

(PCT Rule 24.2(a))

Date of mailing (day/month/year)	IMPORTANT NOTIFICATION
25 October 2000 (25.10.00)	
Applicant's or agent's file reference	**International application No.**
M01/3	PCT/IL00/00555

The applicant is hereby notified that the International Bureau has received the record copy of the international application as detailed below.

Name(s) of the applicant(s) and State(s) for which they are applicants:

M-SYSTEMS FLASH DISK PIONEERS LTD. (for all designated States except US)
MORAN, Dov et al (for US)

International filing date	:	10 September 2000 (10.09.00)
Priority date(s) claimed	:	30 September 1999 (30.09.99) 17 March 2000 (17.03.00)
Date of receipt of the record copy by the International Bureau	:	29 September 2000 (29.09.00)
List of designated Offices	:	

AP :GH,GM,KE,LS,MW,MZ,SD,SL,SZ,TZ,UG,ZW
EA :AM,AZ,BY,KG,KZ,MD,RU,TJ,TM
EP :AT,BE,CH,CY,DE,DK,ES,FI,FR,GB,GR,IE,IT,LU,MC,NL,PT,SE
OA :BF,BJ,CF,CG,CI,CM,GA,GN,GW,ML,MR,NE,SN,TD,TG
National :AE,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BY,CA,CH,CN,CR,CU,CZ,DE,DK,DM,EE,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,NO,NZ,PL,PT,RO,RU,SD,SE,SG,SI,SK,SL,TJ,TM,TR,TT,TZ,UA,UG,US,UZ,VN,YU,ZA,ZW

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No. (41-22) 740.14.35

Authorized officer:

Céline Faust

Telephone No. (41-22) 338.83.38

Continuation of Form PCT/IB/301

NOTIFICATION OF RECEIPT OF RECORD COPY

Date of mailing (day/month/year)	IMPORTANT NOTIFICATION
25 October 2000 (25.10.00)	
Applicant's or agent's file reference	**International application No.**
M01/3	PCT/IL00/00555

ATTENTION

The applicant should carefully check the data appearing in this Notification. In case of any discrepancy between these data and the indications in the international application, the applicant should immediately inform the International Bureau.

In addition, the applicant's attention is drawn to the information contained in the Annex, relating to:

- [X] time limits for entry into the national phase
- [X] confirmation of precautionary designations
- [X] requirements regarding priority documents

A copy of this Notification is being sent to the receiving Office and to the International Searching Authority.

ANNEX TO FORM PCT/IB/301

International application No.
PCT/IL00/00555

INFORMATION ON TIME LIMITS FOR ENTERING THE NATIONAL PHASE

The applicant is reminded that the "national phase" must be entered before each of the designated Offices indicated in the Notification of Receipt of Record Copy (Form PCT/IB/301) by paying national fees and furnishing translations, as prescribed by the applicable national laws.

The time limit for performing these procedural acts is **20 MONTHS** from the priority date or, for those designated States which the applicant elects in a demand for international preliminary examination or in a later election, **30 MONTHS** from the priority date, provided that the election is made before the expiration of 19 months from the priority date. Some designated (or elected) Offices have fixed time limits which expire even later than 20 or 30 months from the priority date. In other Offices an extension of time or grace period, in some cases upon payment of an additional fee, is available.

In addition to these procedural acts, the applicant may also have to comply with other special requirements applicable in certain Offices. **It is the applicant's responsibility** to ensure that the necessary steps to enter the national phase are taken in a timely fashion. Most designated Offices do not issue reminders to applicants in connection with the entry into the national phase.

For detailed information about the procedural acts to be performed to enter the national phase before each designated Office, the applicable time limits and possible extensions of time or grace periods, and any other requirements, see the relevant Chapters of Volume II of the PCT Applicant's Guide. Information about the requirements for filing a demand for international preliminary examination is set out in Chapter IX of Volume I of the PCT Applicant's Guide.

GR and ES became bound by PCT Chapter II on 7 September 1996 and 6 September 1997, respectively, and may, therefore, be elected in a demand or a later election filed on or after 7 September 1996 and 6 September 1997, respectively, regardless of the filing date of the international application. (See second paragraph above.)

Note that only an applicant who is a national or resident of a PCT Contracting State which is bound by Chapter II has the right to file a demand for international preliminary examination.

CONFIRMATION OF PRECAUTIONARY DESIGNATIONS

This notification lists only specific designations made under Rule 4.9(a) in the request. It is important to check that these designations are correct. Errors in designations can be corrected where precautionary designations have been made under Rule 4.9(b). The applicant is hereby reminded that any precautionary designations may be confirmed according to Rule 4.9(c) before the expiration of 15 months from the priority date. If it is not confirmed, it will automatically be regarded as withdrawn by the applicant. There will be no reminder and no invitation. Confirmation of a designation consists of the filing of a notice specifying the designated State concerned (with an indication of the kind of protection or treatment desired) and the payment of the designation and confirmation fees. Confirmation must reach the receiving Office within the 15-month time limit.

REQUIREMENTS REGARDING PRIORITY DOCUMENTS

For applicants who have not yet complied with the requirements regarding priority documents, the following is recalled.

Where the priority of an earlier national, regional or international application is claimed, the applicant must submit a copy of the said earlier application, certified by the authority with which it was filed ("the priority document") to the receiving Office (which will transmit it to the International Bureau) or directly to the International Bureau, before the expiration of 16 months from the priority date, provided that any such priority document may still be submitted to the International Bureau before that date of international publication of the international application, in which case that document will be considered to have been received by the International Bureau on the last day of the 16-month time limit (Rule 17.1(a)).

Where the priority document is issued by the receiving Office, the applicant may, instead of submitting the priority document, request the receiving Office to prepare and transmit the priority document to the International Bureau. Such request must be made before the expiration of the 16-month time limit and may be subjected by the receiving Office to the payment of a fee (Rule 17.1(b)).

If the priority document concerned is not submitted to the International Bureau or if the request to the receiving Office to prepare and transmit the priority document has not been made (and the corresponding fee, if any, paid) within the applicable time limit indicated under the preceding paragraphs, any designated State may disregard the priority claim, provided that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity to furnish the priority document within a time limit which is reasonable under the circumstances.

Where several priorities are claimed, the priority date to be considered for the purposes of computing the 16-month time limit is the filing date of the earliest application whose priority is claimed.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 April 2001 (05.04.2001)

PCT

(10) International Publication Number
WO 01/23987 A1

(51) International Patent Classification[7]: G06F 1/24, 11/30, 17/30, 17/60, G08B 19/02

(21) International Application Number: PCT/IL00/00555

(22) International Filing Date: 10 September 2000 (10.09.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/409,091 30 September 1999 (30.09.1999) US
09/550,491 17 April 2000 (17.04.2000) US

(71) Applicant *(for all designated States except US)*: **M-SYSTEMS FLASH DISK PIONEERS LTD.** [IL/IL]; Kiryat Atidim, P.O. Box 58036, 61580 Tel Aviv (IL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **MORAN, Dov** [IL/IL]; Itamar-Ben-Avi 15, 44406 Kfar Saba (IL). **ELAZAR, Gidi** [IL/IL]; Netafim 2, 44862 Tsur Yigal (IL). **HARKABI, Dan** [IL/IL]; Meshek 17, 79360 Moshav Lahish (IL). **DAN, Raz** [IL/IL]; 30 Borohov Street, Apt. No. 6, 64252 Tel Aviv (IL).

(74) Agent: **BRASS, Daniel**; Plinner, Bodner & Brass, Beit Agish Ravad, 13 Noach Mozes Street, 67442 Tel Aviv (IL).

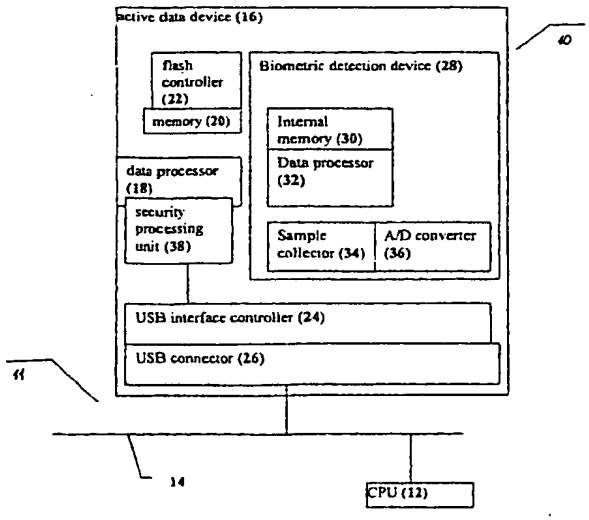
(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

[Continued on next page]

(54) Title: REMOVABLE, ACTIVE, PERSONAL STORAGE DEVICE, SYSTEM AND METHOD



(57) Abstract: A System for providing removable, active, personal storage. The device itself (10) features sufficient computational power (18, 32, 38) and resources (24, 26, 32, 22) to perform various tasks with regard to data storage and retrieval. In particular, these resources are provided such that the management of the memory of the storage device is performed at the device level, rather than requiring management by an external operating system, such as the operating system of an external computational device. At a minimum, the device features a data processor of some type for executing instructions relating to memory management (32), a flash memory device for storing the data and instructions (20), a flash controller for controlling access to a flash memory device (22), a USB controller (24) and a USB connector (26), for connecting the device to an external computational device through the USB bus (14) of the external computational device (12).

WO 01/23987 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL00/00555

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) :G06F 1/24,11/30,17/30,17/60;G08B 19/02
US CL : 707/8;705/41;713/186;340/5.81,5.82;235/379,382
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 707/8;705/41;713/186;340/5.81,5.82;235/379,382

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
DIALOG(COMPSCI,EECOMP,PATENTS)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 4,135,240 A (RITCHIE) 16 January 1979, Abstract, Specification.	1-50
A	US 4,506,329 A (DUWEL et al.) 19 March 1985, Abstract, Specification.	1-50
X	US 4,590,552 A (GUTTAG et al.) 20 May 1986, Column 2, line 3-54; Column 8, line 41 - Column 9, line 20.	1,2,77-12,1 8-22,28,34-40,-47;50
X	US 5,280,527 A (GULLMAN et al.) 18 January 1994; ABstract, Figure 3, Column 2, line 27-65, Column 5, line 34 - Column 6, line 29.	1-50
A	US 5,500,517 A (CAGLIOSTRO) 19 March 1996, Abstract, Figure 3, Figure 4	1-50

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
30 NOVEMBER 2000

Date of mailing of the international search report
29 DEC 2000

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer
PAUL R. LINTZ PH.D. James R. Matthews
Telephone No. (703) 305-3832

Form PCT/ISA/210 (second sheet) (July 1998)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL00/00555

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5,566,327 A (SEHR) 15 October 1996, Abstract, Column 13, lines 27-34.	1-50
A	US 5,719,950 A (OSTEN et al.) 17 February 1998, Abstract, Column 13, line 13-56.	1-50
A	US 5,936,221 A (CORDER et al.) 10 August 1999, Abstract, Specification.	1-50

REMOVABLE, ACTIVE, PERSONAL STORAGE DEVICE, SYSTEM AND METHOD

FIELD AND BACKGROUND OF THE INVENTION

The present invention relates to a device, a system and method for removable, active, personal storage, and in particular for such a device, system and method which are suitable for operation with multiple computational devices at remote access points.

Computers are useful for the storage, retrieval and manipulation of data. Currently, many different types of electronic data storage devices are used in conjunction with computers. These electronic storage devices may be located externally or internally to the computer with which the storage device is in communication. For example, a magnetic storage device, such as hard disk drive, could be located internally to the computer, in direct communication with the system bus of the computer and operated by the CPU (central processing unit) of the computer. Flash memory, which is both readable and writable non-volatile memory, is a physically smaller storage device, which may be located within the physical case of the computer, and which is also connected to the system bus and operated by the CPU.

Removable storage media may also be used to store data, in which a hardware device, or "drive", for reading from and/or writing to the storage medium, is connected to the system bus of the computer. Examples of removable storage media include, but are not limited to, optical disks, CD-ROM disks and floppy diskettes. At some level, all of these various hardware devices are in communication with the computer which operates the device, regardless of the location of the electronic storage device. Therefore, access to the data is provided through such a computer.

There are a number of important aspects for data storage, particularly given the prevalence of communication through the Internet. First, data storage should be secure. Second, data storage should be accessible at multiple locations, such that the user can access the data at more than one access point. Unfortunately, these two goals are directly contradictory, as permitting access to the data from multiple access points significantly decreases the security of the data. A third important aspect of data storage is personalization, such that the user who owns the data is able to access it quickly and easily, yet such access is blocked to other, non-authorized users. None of these aspects is satisfied by currently available solutions which are known in the art.

As an example, with regard to data security, currently, most forms of data access control are implemented as software programs, which have a number of disadvantages. For example, these programs may be "hacked" or overcome by an unauthorized user, who can then gain access

to the data. Such a disadvantage has become more acute with the advent of networks, distributed data storage and "client-server" applications, all of which increase the number of access points to the computer through which the electronic storage device is accessed, and hence to the stored data on that device. Such an increased number of access points also potentially increase the ability of an unauthorized user to access the data. Thus, software programs are clearly not adequate protection for data stored in a networked environment with multiple access points.

Another type of data access control is provided through the operating system of the computer itself. For example, UNIX and other operating systems typically allow an authorized user to determine the level of permissions associated with a particular file and/or sub-directory, which could be "read-only", "read/write" and so forth. Unfortunately, such permissions are often relatively simple, only differentiating between "read" and "write" for example. Also, like other types of software programs, these operating systems may be "hacked" by an unauthorized user, who can then gain access to the data.

In addition, if the electronic hardware storage device itself is stolen, then typically the data becomes completely unprotected, such that any unauthorized user can easily gain access to the data on the storage device. Neither software programs nor the operating system of the computer can overcome this problem, since they are stored and implemented separately from the storage device itself.

A more useful solution would be implemented with the hardware of the electronic storage device in a more integrated manner, such that even if the storage device itself is stolen, the data could not be easily accessed. Furthermore, such integration would increase the difficulty of access by an unauthorized user, whether to a network or to the local storage device itself. Furthermore, such a device should be portable, so that the user could transport the device and retrieve the data at remote locations. The overall solution should also permit personalization of the data storage and retrieval functions. Unfortunately, such a solution is not currently available.

There is thus an unmet need for, and it would be useful to have, a device, a system and a method for removable, active, personal storage, which does not rely on separately stored software programs, which is optionally integrated with the hardware of the storage device, and which is highly portable for use by the user at multiple locations.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and other objects, aspects and advantages will be better understood from the following detailed description of a preferred embodiment of the invention with reference to

the drawings, wherein:

FIG. 1 is a schematic block diagram of an exemplary system according to the present invention;

FIG. 2 is a schematic block diagram of a preferred embodiment of a system according to the present invention;

FIG. 3 is a flowchart of an exemplary method for operating the system of Figure 2 according to the present invention;

FIG. 4 shows another embodiment of the present invention, for an access control device for controlling access to data; and

FIG. 5 shows a flowchart of an example of a method according to the present invention, with regard to access to data in the form of a stored credit card number.

SUMMARY OF THE INVENTION

The present invention is of a device, a method and a system for providing removable, active, personal storage. The device itself features sufficient computational power and resources to perform various tasks with regard to data storage and retrieval. In particular, these resources are provided such that the management of the memory of the storage device is performed at the device level, rather than requiring management by an external operating system, such as the operating system of an external computational device for example.

At a minimum, the device features a data processor of some type for executing instructions related to memory management, a flash memory device for storing the data and instructions, and some type of connector for connecting the device to an external computational device. For example, such a connection could optionally be made with a USB controller and a USB connector at the device, for connecting the active device through the USB bus of the external computational device. Alternatively, the connection could optionally be made through a Bluetooth-enabled transceiver at the device itself and at the external computational device. Preferably, the present invention is implemented as an active data device, such as a chip for example, which more preferably controls access to the network. This implementation is preferred, since such electronic devices are more difficult to "hack" for access by an unauthorized user.

The device of the present invention may optionally be implemented in a number of different ways, all of which are considered to be within the scope of the present invention, including but not limited to, devices connected to a computer through any suitable hardware

connection interface; a single chip with a microprocessor and firmware for operating the access features.

According to the present invention, there is provided a device for controlling access to a resource, access being provided through a host device having a USB bus, the device comprising: (a) an input for receiving a request to access the resource; (b) a flash memory device for storing at least one permission for determining access to the resource; (c) a flash memory controller for controlling said flash memory device; (d) a processor for executing said at least one instruction and for comparing said request to said at least one permission, such that if said at least one permission includes a type of access requested in said request, access to the resource is provided, and alternatively if said at least one permission does not include a type of access requested in said request, access to the resource is not provided; and (e) a USB interface controller for communicating with the USB bus of the host device and, if permitted, for transmitting data from said processor.

Hereinafter, the terms "computer user" and "user" both refer to the person who operates a computer which is in communication with a data storage device.

Hereinafter, the term "computer" refers to a combination of a particular computer hardware system and a particular software operating system. Examples of such hardware systems include those with any type of suitable data processor. Hereinafter, the terms "computer" or "computational device" include, but are not limited to, personal computers (PC) having an operating system such as DOS, Windows™, OS/2™ or Linux; MacOS™, Macintosh™ computers; computers having JAVA™-OS as the operating system; and graphical workstations such as the computers of Sun Microsystems™ and Silicon Graphics™, and other computers having some version of the UNIX operating system such as AIX™ or SOLARIS™ of Sun Microsystems™; a PalmPilot™, a PilotPC™, or any other handheld device; any other device featuring known and available operating system; as well as any type of device which has a data processor of some type with an associated memory. Hereinafter, the term "Windows™" includes but is not limited to Windows95™, Windows NT™, Windows98™, Windows CE™ Windows 2000™, Windows ME™ and any upgraded versions of these operating systems by Microsoft Corp. (USA).

Hereinafter, the term "biometric detection device" refers to any type of device which is capable of capturing data with regard to a biological parameter of a user, including, but not limited to, a fingerprint detection device and a device which performs a retinal scan.

For the present invention, a software application could be written in substantially any

suitable programming language, which could easily be selected by one of ordinary skill in the art. The programming language chosen should be compatible with the computer by which the software application is executed, and in particularly with the operating system of that computer. Examples of suitable programming languages include, but are not limited to, C, C++ and Java. Furthermore, the functions of the present invention, when described as a series of steps for a method, could be implemented as a series of software instructions for being operated by a data processor, such that the present invention could be implemented as software, firmware or hardware, or a combination thereof.

DETAILED DESCRIPTION OF THE INVENTION

The present invention is of a device, a method and a system for providing removable, active, personal storage. The device itself features sufficient computational power and resources to perform various tasks with regard to data storage and retrieval. In particular, these resources are provided such that the management of the memory of the storage device is performed at the device level, rather than requiring management by an external operating system, such as the operating system of an external computational device for example. At a minimum, the device features a data processor of some type for executing instructions related to memory management, a flash memory device for storing the data and instructions, a flash controller for controlling access to a flash memory device and some type of connector for connecting the device to an external computational device. For example, such a connection could optionally be made with a USB controller and a USB connector at the device, for connecting the active device through the USB bus of the external computational device. Alternatively, the connection could optionally be made through a Bluetooth-enabled transceiver at the device itself and at the external computational device.

Optionally and preferably, the present invention also features an authenticator, for identifying and authenticating the user. Such an authenticator may optionally and more preferably feature a biometric detection device, which collects a biological parameter of the user in order to identify the user. Examples of different types of biological parameters which optionally could be collected with such a biometric detection device include, but are not limited to, fingerprint, face image recognition, retinal print, iris image analysis, hand geometry, voice analysis, ear shape, detection of odor of the user, palm print and finger geometry. Once the biological parameter has been collected, in a step which is also termed "enrollment", the biological parameter data is analyzed. This analysis involves the extraction of at least one, and

system of the host computational device. A specific driver for memory management of the device of the present invention, operated by the operating system of the host computational device, is not required since the device of the present invention performs housekeeping and other memory management functions locally. Thus, the present invention is far more flexible than other devices which are known in the art, as these latter known devices cannot provide the active device functions of the present invention.

The principles and operation of a device, a system and a method according to the present invention may be better understood with reference to the drawings and the accompanying description, it being understood that these drawings are given for illustrative purposes only and are not meant to be limiting.

Referring now to the drawings, Figure 1 is a schematic block diagram of an illustrative, exemplary system according to the present invention for controlling data access. A system **10** features a computational device **11** which contains a CPU **12** for executing instructions, such as a request to read data for example. System **10** also features other computational devices **17** connected to computational device **11** through a network.

CPU **12** is connected to a bus **14**. An active data device **16** is also connected to bus **14**, such that active data device **16** is in communication with CPU **12** through bus **14**. Bus **14** is preferably a USB (universal serial bus), although of course bus **14** may alternatively be implemented as any other suitable type of bus connection.

The user is preferably identified and authenticated by active data device **16**, which then determines the type of access permitted to the user. Such access may optionally include access to local data storage of active data device **16** (not shown; see Figure 2), and/or to one or more resources of computational device **11** (not shown). Generally, active data device **16** preferably determines whether the user is able to access information stored in the local storage of active data device **16**, computational device **11**, or other computational devices **17**.

Active data device **16** is optionally implemented according to any one of a plurality of different specific embodiments. For example, active data device **16** could optionally be implemented as a chip, with a non-volatile memory which is both readable and writable, such as a flash memory device for example, some type of input for receiving a request for data, and a microprocessor. The chip is preferably implemented as a programmable ASIC.

Figure 2 shows a more detailed schematic block diagram of an exemplary implementation of active data device **16**. Active data device **16** features a data processor **18**, which operates instructions for controlling the functions of active data device **16**, as well as for

communicating with host external computational device **11**. Data processor **18** reads these instructions from a memory component **20**, which is preferably a flash memory device. In the preferred implementation, memory component **20** is controlled by a flash controller **22**, which in turn receives commands from data processor **18** regarding access to the stored information in memory component **20**.

Memory component **20** more preferably features instructions for memory management, such that data processor **18** is able to manage memory component **20** through flash controller **22**, most preferably without requiring any type of management from an external computational device such as host external computational device **11**. One example of a suitable memory management system for a flash memory is disclosed in US Patent No. 5,404,485, entitled "Flash File System", which is hereby incorporated by reference as if fully set forth herein.

According to a preferred embodiment of the present invention, memory component **20** also serves for storing data for the user, apart from data which is stored in order to facilitate the operation of active data device **16**. Memory component **20** thus preferably acts as a local data storage device for the user, with the stored data being accessed by the user through commands sent to data processor **18**. Optionally memory **20** is external to active device **16** ASIC.

Active data device **16** communicates to external devices, such as host computational device **11**, through a USB interface controller **24** and a USB connector **26**. USB interface controller **24** and USB connector **26** in turn communicate with CPU **12** through USB bus **14**, for transmitting and receiving data.

The operation of these components of active data device **16** may optionally be performed as follows. Once the correct type of access for the user has been determined, active data device **16** communicates with CPU **12** of computational device **11** through USB bus **14**. In this case, computational device **11** is the USB host, while active data device **16** is considered to be a slave device, such that only computational device **11** is empowered to initiate a communication session. Active data device **16** features USB interface controller **24**, which is a chip for translating digital data into analog signals. These signals are then sent through USB connector **26** to USB bus **14**. USB connector **26** is optionally and more preferably implemented as a flexible connector, such that USB connector **26** can be connected to USB bus **14** regardless of the structure and layout of the surrounding ports, for other connectors and peripheral devices. In addition, USB connector **26** according to the present invention more preferably features a protector of some type, in order for USB connector **26** to be kept without being damaged or accumulating dirt.

The operation of the internal components of active data device **16** with regard to computational device **11** is optionally and preferably performed as follows, it being understood that this is only one exemplary method for performing such an interaction. First, data processor **18** initializes USB interface controller **24**, as well as memory component **20**, and optionally a security processing unit **38** and/or a biometric detection device **28**, as described in greater detail below. Next, USB interface controller **24** waits for an initialization signal from computational device **11**, which is the host device. Once the initialization signal has been received, data from computational device **11** is accepted.

As such data is transmitted, USB interface controller **24** signals data processor **18** that a message has been received. Data processor **18** then receives and analyzes the message. Data processor **18** performs one or more actions, as required by the contents of the message, and data is prepared for USB interface controller **24** to return to computational device **11**.

Depending upon the contents of the message from computational device **11**, data processor **18** may process and store data in memory component **20**, for example, if the message contained a command to store data at active data device **16**. Alternatively, as commanded by computational device **11**, data processor **18** may read data from memory component **20**, and then send the read data to USB interface controller **24** for transmission to computational device **11**.

According to optional but preferred embodiments of the present invention, active data device **16** features biometric detection device **28** for the purpose of identifying a user. As for Figure 1, access to computational device **11**, as well as to an optional local data storage of active data device **16** at memory **20**, as previously described, is provided through active data device **16**. However, active data device **16** now determines access to computational device **11** and optionally local data storage according to the biological parameter of the user, which is measured by biometric detection device **28** for the purpose of identifying the user.

Biometric detection device **28** is optionally implemented according to a plurality of different embodiments. For example, biometric detection device **28** could be implemented as a fingerprint detection device or as a retinal scanning device. As a fingerprint detection device, biometric detection device **28** is optionally and preferably implemented as a FingerChip™ (Thomson-CSF Semiconducteurs Specifiques, France; see *www.tcs.thomson-csf.com/Us/fingerchip/fc_home.htm* as of March 23, 2000). Biometric detection device **28** optionally and preferably contains an internal memory **30** for storing instructions on the scanning of fingerprints, and more preferably on the interpretation of such fingerprints with regard to stored fingerprint data. The stored fingerprint data is also optionally

stored on internal memory **30**, but alternatively is stored on memory component **20** of active data device **16**. If biometric detection device **28** contains internal memory **30**, then more preferably a data processor **32** is also present.

Biometric detection device **28** also includes a sample collector **34** for collecting a sample of the biological parameter. For example, for a fingerprint detection device, sample collector **34** preferably includes a thermal imaging fingerprint sensor for collecting the fingerprint data, as described in greater detail below. The fingerprint data is then optionally analyzed by biometric detection device **28**, and more specifically by a software module which is stored in internal memory **30** and which is operated by data processor **32**. Alternatively, the fingerprint data is analyzed by a software module being operated by active data device **16**. Similarly, a retinal scan could be collected with sample collector **34**, optionally implemented as a light scanner which is suitable for transmitting light into the eye of the user.

In an exemplary embodiment with the FingerChip™ device, sample collector **34** is optionally implemented with this device. The FingerChip™ device is a small silicon chip (smaller than the size of the fingertip), which is a thermal imaging sensor. Other types of sensors for collecting fingerprint data include, but are not limited to, optical sensors which use light in conjunction with a scanning device such as a CCD (charge-coupled device) camera for example; devices which sense capacitance; and combinations of such sensors (see *www.tcs.thomson-csf.com/fingerchip/DownloadFAQ/faq.htm* as of March 23, 2000 for an explanation of the different devices, including the FingerChip™ device itself). Such a chip can optionally be connected to an analog-to-digital (A/D) converter **36** for converting the analog thermal signal to a digital signal. The digital signal is then optionally passed to data processor **32** for analysis, as described in greater detail below.

Once the biological parameter has been collected from the user and analyzed, the specific identity of the user can optionally be determined. Such a specific identity can then be used to determine the type of access which is to be granted to the user. Such access is preferably determined through the operation of data processor **18** for active data device **16**, which preferably reads one or more instructions which are stored on memory component **20**. These instructions contain information for correlating the identity of the user to various types of access which should be given to the user, optionally with a user profile for determining the preferences of the user for interacting with computational device **11** and/or local data storage provided through memory component **20**.

As previously described, if memory component **20** is a flash ROM device, preferably

memory component **20** features flash controller **22** for controlling interactions between data processor **18** and memory component **20**. Optionally and more preferably, memory component **20** may also include a RAM (random access memory) device, to enable data processor **18** to perform the instructions contained on memory component **20**, as well as to act as a communication buffer.

According to preferred embodiments of the present invention, active data device **16** features a security processing unit **38**. Security processing unit **38** features an encryption engine for optional encryption of data which is transmitted to computational device **11**, and decryption of any encrypted data which may be received from computational device **11**. Security processing unit **38** features an authentication engine for storing authentication code(s) for the owner of the device. The authentication engine can participate in such an authentication process. Security processing unit **38** optionally features an authenticity algorithm which can affirm the authenticity of data. Security processing unit **38** is optionally and preferably implemented as a hardware device, such as chip, for more rapid performance and a more secure implementation of the encryption/decryption procedures.

Figure 3 is a flowchart of an exemplary method according to the present invention for the operation of the preferred system of Figure 2. This method is explained with regard to the detection of a fingerprint as a biological parameter for the purposes of illustration only and without any intention of being limiting. In addition, the method is also explained with regard to the use of the present invention for determining access to a network resource only for the purposes of illustration, and again without any intention of being limiting.

In step 1, the user connects the USB connector of the active data device to the host computational device. It should be noted that the active data device is preferably highly portable, such that the user could easily carry the active data device to each host computational device to which the active data device is to be connected.

In step 2, the active data device performs a handshake procedure with the host computational device, through the USB interface of the active data device and the USB bus of the host computational device, as previously described.

In step 3, according to preferred embodiments of the present invention, the user places a finger in proximity to the biometric detection device, in order to gain access to the requested network resource. For example, with regard to the FingerChip™ device, as described in greater detail above, the finger of the user is swept over the surface of the chip such that at least the pad of the fingertip of the user touches this chip.

In step 4, the biometric detection device detects the presence of the finger of the user in order to begin the collection procedure. For example, with regard to the FingerChip™ device, the presence of the fingertip is sensed by a thermal sensor, such that a sharp alteration in the thermal pattern indicates that the fingertip of the user is in proximity to the device (see *www.tcs.thomson-csf.com/fingerchip/description/reconstr.htm* as of March 23, 2000 for an explanation of the entire detection and data collection procedure). Of course, other implementations of such a device may optionally employ alternate mechanisms.

In step 5, the data related to the biological parameter of the user is collected by the sample collector of the biometric detection device. For example, data acquisition may involve the collection of one or more images, such as the thermal images of the FingerChip™ device. Each such image is of at least a portion of the fingertip of the user. Optionally and preferably, a plurality of images are collected.

In step 6, the data is analyzed in order to determine whether the collected biological parameter of the user is a sufficiently close match to the stored identification information of a permitted user. The user is presumed to have provided a measurement of such a biological parameter previously, in order for this information to be stored for later comparison.

For example, for fingerprint detection, preferably the plurality of images (if collected) are assembled to form a single image. Next, the assembled image is analyzed for pattern detection, in order to compare at least one, and preferably a plurality of, points of similarity to the stored data.

In step 7, the biometric detection device, or alternatively the active data device if the two devices are implemented separately, determines whether the collected biological parameter is sufficiently similar to a stored pattern with the requisite permission, in order for the user to be granted access to the network resource. Optionally, a log may be kept of access attempts, and/or of unsuccessful access attempts.

In step 8, if the collected biological parameter is sufficiently similar to the stored pattern, then the user is given permission to access the requested data, such as at the host computational device and/or at the local data storage on the active data device itself. Alternatively, the user is not given permission to access the requested information, if the collected biological parameter is not sufficiently similar.

If the user is given permission to access the requested information, then in step 9, the data is retrieved, either from the local memory storage of the active data device, or alternatively from the data storage of the host computational device. Optionally and more preferably, the user may

be given differential permission to access different types of data. More preferably, such differential permission is compared to the identification information about the user, such that the active data device is able to determine whether the user can perform the requested type of access on the particular data.

According to preferred embodiments of the present invention, the user may choose to transmit or receive encrypted data, in step 10. For example, if the user wants to send data from the local memory of the active data device to the host computational device, such data is optionally and more preferably encrypted by the active data device before being sent to the host computational device.

Optionally, in addition to the identification procedure described above, an authentication procedure is also performed for authenticating the user to the host computational device, for example. In this procedure, the identity of the user is preferably sent to the host computational device, optionally and more preferably with an authentication code. The host computational device then examines the identification and optional authentication code information, to determine if the user should be given access to one or more computational resources. If the host computational device authenticates the user according to the provided information, then the user is permitted access to one or more computational resources. Most preferably, the authentication process involves a multiple part handshake procedure between the active device and the host computational device, for a more secure authentication procedure. Optionally, the authentication process may also include authentication of the active device to a system, including a handshake procedure between a remote computational device, the active device and the host computational device. The remote computational device may be connected to the host computational device through the Internet.

Bluetooth is a standard for a wireless digital communications technology which is based on radio frequency (RF) transmission. Bluetooth is intended to interconnect computational devices such as home computers, hand held devices and peripherals. Therefore, the standard requires low power consumption, such that a relatively short-range connection between the receiver and the transmitter is also required.

Bluetooth devices are organized into networks, called "piconets", which contain small groups of such devices. A device which implements the Bluetooth technology, termed herein a "Bluetooth device", may be a master or a slave in a network of such devices. A piconet has one master device, and one or more slave devices which receive commands from the master device. A device may optionally belong to more than one piconet. A piconet is synchronized to a pattern

of frequencies, in which all devices in the piconet communicate at the same frequency for a predetermined period of time, after which all devices transfer communication to the next frequency in the pattern. The master device chooses the frequency pattern to be used.

The Bluetooth standard features a discovery protocol for the dynamic formation of each particular Bluetooth network. The master device initiates the discovery process in order to locate other available slave devices. After a connection is established and the network has been formed, digital data can be transferred between the devices through the network.

Figure 4 shows another embodiment of the present invention, for an access control device for controlling access to data. This embodiment of the present invention may be active or passive, in that this embodiment may be composed of components which rely upon the management and control of the host computational device. Furthermore, such a device may optionally be implemented with the biometric detection device of Figure 2, according to the method of Figure 3. Alternatively or additionally, the device could be implemented with either Bluetooth or USB communication, as previously described.

As for Figure 1, a system **40** features a CPU **42** for executing instructions, such as a request to read data for example. CPU **42** is connected to a bus **44**. An access control device **46** is also connected to bus **44**, such that access control device **46** is in communication with CPU **42** through bus **44**. Bus **44** is preferably a USB (universal serial bus), although of course bus **44** may alternatively be implemented as any other suitable type of bus connection.

A data storage device **48** is in communication with access control device **46**, such that any attempts to access data in data storage device **48** must pass through access control device **46**. Preferably, as shown, data storage device **48** is not in direct communication with bus **44**. Therefore, if CPU **42** receives an instruction to read data from data storage device **48**, CPU **42** preferably cannot directly read such data by sending a command through bus **44** directly to data storage device **48**. Rather, preferably CPU **42** must send the command to access control device **46**, which then determines if such access should be granted and the data read from data storage device **48**. Thus, more preferably, data can only be read from, and written to, data storage device **48** through access control device **46**.

Access control device **46** is optionally implemented according to a plurality of different embodiments, at least partially determined by the particular type of data storage device **48**. For example, access control device **46** could optionally be implemented as a chip, with a non-volatile memory which is both readable and writable, such as a flash memory device for example, some type of input for receiving a request for data, and a microprocessor. As described in greater

detail below, the various types of permissions could optionally be stored on the non-volatile memory, along with a set of instructions operated by the microprocessor. The chip could also be implemented as a programmable ASIC.

When access control device **46** receives a request for particular data which is stored in data storage device **48**, the stored instructions are executed by the microprocessor in order to compare the request for the data to the stored permissions. If the stored permissions are such that the data request may be fulfilled, as described in greater detail below, then access control device **46** enables data to be retrieved from data storage device **48**. Otherwise, access control device **46** does not enable the data to be retrieved. Since preferably data storage device **48** can only be accessed through access control device **46**, if such access is not granted by access control device **46**, then the data cannot otherwise be retrieved.

Access control device **46** could also optionally be directly integrated into data storage device **48**. For example, if data storage device **48** is a flash memory device, which is typically embodied as a chip, then the functions of access control device **46** could be integrated into the chip itself. For example, data storage device **48** could be incorporated into a single chip with a microprocessor for access control device **46**, and firmware for operating the data access features. Alternatively, access control device **46** may optionally only feature logic, such that access control device **46** would interact with CPU **42** for operating software for interacting with the logic, and hence for performing the data access method of the present invention. Alternatively, access control device **46** and data storage device **48** may be implemented as a plurality of separate functional units which are not combined in a single chip.

However, the implementation of access control device **46** as a chip, or other electronic device, whether integrated into, or separate from, data storage device **48**, is particularly preferred since such an implementation also enables the security of access control device **46** to be more easily maintained, as electronic hardware devices are more difficult to "hack" for unauthorized access. As described above, access control device **46** is preferably implemented as firmware, which combines software instructions stored on a hardware memory, with additional hardware components such as a microprocessor for performing the instructions.

According to preferred embodiments of the present invention, system **40** enables a plurality of different types of permissions for accessing data to be stored by access control device **46**, such that a variety of different types of data access can be provided. As an example, one type of permission could be a standard read and write permission, but with write protection, such that access control device **46** would permit data to be read from data storage device **48**, but

would block an attempt to write data to data storage device **48**. If such a permission is to be stored in an abbreviated code, the code for this particular type of permission could be given as "R/W/WP", for example. Such a code could optionally be stored in the non-volatile memory of access control device **46**, for example. However, the permission is such that it could be changed to permit such write access, or a read and write permission with no write protection, with a code as follows: R/W/NP. These standard types of read and write permissions are often used for hard disks, floppy diskettes and other storage media, for example.

The present invention also preferably enables more complex types of permissions to be implemented. For example, the permission could be given as "write once and read many times", or "WO/RM" in code form, such that the data could only be written to data storage device **48** once, but could be read from data storage device **48** many times. One example of a useful implementation of such a permission is the storage of a picture for identifying a user, for example in order to permit access to a particular location.

Another type of optional but preferred implementation of a permission is "write once, no read, comparison with yes/no answer only", or "WO/NR/C" in code form. This type of permission indicates that the data can only be written to data storage device **48** once and cannot be read from data storage device **48**. However, access control device **46** can enable the data to be compared with received data, but would only provide information in the form of a "yes" or "no" answer as a result of the comparison. One example of a useful implementation of such a permission is for a PIN (personal identification number) or other number for identifying a user, such as for accessing a bank account or using a credit card. Access control device **46** can receive data in the form of the PIN or other information entered by the user, and can then compare the received data to data which is stored in data storage device **48**. Access control device **46** would then confirm whether the correct PIN or other identification information had been entered by returning a positive or negative comparison. The stored data would not be released from data storage device **48**, such that the PIN could not be read from data storage device **48** by an unauthorized user. Thus, data security would be maintained, while still enabling the identity of the user to be confirmed according to an entered PIN or other identification information.

One variation of this type of permission incorporates permission, or lack thereof, for updating the stored data. With regard to the example above, the PIN or other identification information could optionally be changed for updating, if the permission is given as updatable, or WO/NR/C/U in code form. Alternatively, if the permission is given such that the data cannot be updated, or WO/NR/C/U in code form, then the data cannot be altered.

A more specific example of these different types of permissions, and their use thereof, is given below with regard to Figure 5, which features a flowchart of an illustrative and exemplary method according to the present invention for controlling data access.

Figure 5 shows a flowchart of an example of a method according to the present invention, with regard to access to data in the form of a stored credit card number. In step 1, a plurality of different types of information are combined to form the credit card number. Preferably, the format of the credit card number is given as follows:YYYZZZDDDAAA, in which YYY is a code which identifies the originator of the credit card data, such as the provider of the credit card; ZZZ is an identification number for the credit card account, which currently forms the credit card number in background art implementations of a credit card; DDD, which optionally features other data about the credit card account, such as the date when the credit card was issued, where the credit card was issued, the expiration date and so forth; and AAA, which optionally and preferably is a PIN as previously described.

In step 2, each portion of the credit card number is stored with a separately selected and assigned data access permission, which optionally and preferably is different for each portion of the number. For example, preferably "YYY", "ZZZ" and "DDD" are each stored with the permission assigned as WO/RM (write once, read many times); AAA is preferably stored with the permission assigned as WO/NR/C/U (write once, do not read, compare only, updatable). These permissions are described in greater detail above.

In step 3, the user attempts to purchase a product with the credit card number. In step 4, the merchant or other party receiving the payment enters the credit card number. It should be noted that this step is optionally performed substantially automatically, for example for e-commerce through a Web site. In step 5, the access control device receives the credit card number.

In step 6, the access control device determines the type of permission for each portion of the credit card number. In step 7, the access control device performs the commands which are permitted, optionally including reading the portions of the credit card number which are designated as "YYY", "ZZZ" and "DDD", and performing a comparison with the portion of the credit card number which is designated as "AAA". In step 8, the permitted information is returned by the access control device. Thus, this illustrative method is an example of the utility of the present invention for validating a credit card number for performing a purchase.

Other types of data which could be stored with an assigned type of permission according to the present invention include, but are not limited to, an access control code, an identification

code and various types of data files, as described in greater detail below.

For example, an access control code could be implemented with a combination of different types of data, each of which could again feature a separately selected and assigned data access permission, which optionally and preferably is different for each portion of the data. If the access control code is implemented as a number, then preferably these different types of data are as follows, with the data access permissions. The first portion of the access control code is optionally a code which identifies the data as an access control code, and which is preferably stored as "WO/RM". The second portion of the access control code is preferably the access code itself, and is preferably stored as "WO/NR/C/U".

Similarly, an identification code is optionally and preferably composed of a first portion which identifies the data as an identification code, and which is preferably stored as "WO/RM", and a second portion which is the unique identification code, for example for a hardware device, which is preferably stored as "WO/RM".

Other types of data files may be stored with associated permission types as desired, which are constructed as previously described. For example, most data files are preferably stored as "R/W" data, with the decision to permit writing to the data ("R/W/WP") or not to permit such writing ("R/W/NP"), decided according to user preference. Thus, the present invention can accommodate many different types of uses for the control of data access.

According to another optional embodiment of the present invention, data could be stored on the storage device according to a data access type which may be defined as "read a few times, then delete". According to this preferred type of data access, a file would be stored on the device of the present invention and could then be read only a predefined number of times, which preferably would be a plurality of different read times. After the data had been read the predefined number of times, the device of the present invention would then delete the data, or otherwise render the data inaccessible for an additional data read. This type of data access is preferred for file types such as MP3 music files, which may be provided by a vendor for only such a predefined number of data read accesses, for example in order to prevent the unauthorized redistribution of such files.

For any of the embodiments of Figures 1-5, optionally and preferably, the device features a modified user interface. More preferably, the device of the present invention does not feature a keyboard or a display screen. Instead, the device more preferably communicates with the user through audio data, such as through synthesized human speech for example. Additionally or alternatively, the device preferably provides information concerning the state of device operation

with a LED, for example. Optionally and most preferably, the device is able to communicate more information about the state of device operation by sending an e-mail message or triggering the host computational device to send an e-mail message to a predetermined e-mail address. Thus, the device of the present invention is most preferably able to communicate with the user without a GUI (graphical user interface).

It will be appreciated that the above descriptions are intended only to serve as examples, and that many other embodiments are possible within the spirit and the scope of the present invention.

WHAT IS CLAIMED IS:

1. A device for controlling access to a resource, access being provided through a host device having a USB bus, the device comprising:

(a) an input for receiving a request to access the resource;

(b) a flash memory device for storing at least one permission for determining access to the resource;

(c) a flash memory controller for controlling said flash memory device;

(d) a processor for executing said at least one instruction and for comparing said request to said at least one permission, such that if said at least one permission includes a type of access requested in said request, access to the resource is provided, and alternatively if said at least one permission does not include a type of access requested in said request, access to the resource is not provided; and

(e) a USB interface controller for communicating with the USB bus of the host device and, if permitted, for transmitting data from said processor.

2. The device of claim 1, wherein the device is implemented as a programmable ASIC.

3. The device of claim 1, wherein access is determined according to a biological parameter of a user, the device further comprising a biometric detection device for detecting said biological parameter of the user and for determining whether the user has said at least one permission to access the stored data, said biometric detection device being connected to said processor.

4. The device of claim 3, wherein said biometric detection device further comprises:

(i) a sample collector for collecting said biological parameter of the user; and

(ii) a software module for analyzing said biological parameter to determine whether the user has said at least one permission to access the resource.

5. The device of claim 4, wherein said biometric detection device further comprises:

(iii) a memory device for storing said software module and at least one previously collected biological parameter of the user; and

(iv) a data processor for operating said software module.

6. The device of claim 5, wherein said biological parameter of the user is a fingerprint of the user.

7. The device of claim 1, further comprising:

(f) a RAM component for storing data for performing said at least one instruction of said data processor.

8. The device of claim 1, further comprising:

(f) a cryptographic chip for encrypting and decrypting data.

9. The device of claim 8, wherein said cryptographic chip performs an authentication process.

10. The device of claim 8, wherein said cryptographic chip emulates a smart card.

11. The device of claim 10, wherein said cryptographic chip stores encrypted smart card data.

12. The device of claim 8, wherein said cryptographic chip performs encryption immediately upon receiving a command from said data processor.

13. The device of claim 12, wherein said cryptographic chip creates a cryptographic signature with a hash immediately upon receiving a command from said data processor.

14. The device of claim 8, wherein said cryptographic chip further comprises a cryptographic chip memory for storing at least one cryptographic key and at least one cryptographic instruction for encrypting and decrypting data, such that said cryptographic chip forms a removable encryption engine.

15. The device of claim 14, wherein said encrypted data is stored on said cryptographic chip memory.

16. The device of claim 15, wherein said cryptographic chip memory is a separate flash memory device from said flash memory device.

17. The device of claim 15, wherein said cryptographic chip memory is said flash memory device.

18. A system for controlling access to a network resource, the system comprising:

(a) an active data device for controlling access to the network resource, said active data device featuring a USB (universal serial bus) interface controller;

(b) a host computational device for communicating with said active data device to provide access to the network resource, said host computational device featuring a USB bus for communicating with said USB interface controller for data exchange with said active data device; and

(c) a network for connecting said host computational device to the network resource.

19. The system of claim 18, wherein said active data device further comprises firmware for storing a plurality of instructions and a data processor for performing said plurality of instructions, such that said active data device determines said access according to said instructions of said firmware.

20. The system of claim 18, wherein said active data device is implemented as a programmable ASIC.

21. The system of claim 18, wherein said active data device further comprises:

(i) a non-volatile memory for storing at least one instruction for determining access to the network resource; and

(ii) a processor for executing said at least one instruction to determine if access is to be provided to the network resource.

22. The system of claim 21, wherein said non-volatile memory is a flash memory device, such that said active data device further comprises a flash controller for being controlled

by said processor.

23. The system of claim 18, wherein access is determined according to a biological parameter of a user and said active data device further comprises a biometric detection device for detecting said biological parameter of the user and for determining whether said user has permission to access the network resource.

24. The system of claim 23, wherein said biometric detection device further comprises:

(i) a sample collector for collecting said biological parameter of the user; and

(ii) a software module for analyzing said biological parameter to determine whether said user has said permission.

25. The system of claim 24, wherein said biometric detection device further comprises:

(iii) a memory device for storing said software module and at least one previously collected biological parameter of the user; and

(iv) a data processor for operating said software module.

26. The system of claim 25, wherein said biological parameter of the user is a fingerprint of the user.

27. The system of claim 18, further comprising:

(d) a cryptographic chip on said active device for encrypting and decrypting data, such that access to said host computational device is determined according to an authentication procedure performed with said cryptographic chip.

28. A method for controlling access to a resource, access being provided through a host device having a USB bus, the method comprising the steps of:

(a) providing an active data device for determining access to the resource, said active data device featuring an USB interface controller;

(b) receiving a request to access the resource by said active data device;

(c) comparing said request to at least one permission for determining access to the

resource by said active data device;

(d) if said at least one permission includes a type of access requested in said request, sending said request from said active data device to the USB bus of the host device through said USB interface controller;

(e) providing access to the resource through the host device; and

(f) alternatively, if said at least one permission does not include said type of access requested in said request, rejecting said request by said active data device.

29. The method of claim 28, wherein access is determined for a user and wherein step (b) further comprises the steps of:

(i) collecting a biological parameter of said user; and

(ii) analyzing said biological parameter to determine an identity of said user, such that said at least one permission is determined according to said identity.

30. A device for controlling access to a resource, access being provided through a host device having a radio transceiver, the device comprising:

(a) an input for receiving a request to access the resource;

(b) a flash memory device for storing at least one permission for determining access to the resource;

(c) a flash memory controller for controlling said flash memory device;

(d) a processor for executing said at least one instruction and for comparing said request to said at least one permission, such that if said at least one permission includes a type of access requested in said request, access to the resource is provided, and alternatively if said at least one permission does not include a type of access requested in said request, access to the resource is not provided;

(e) a device radio transceiver for communicating with the radio transceiver of the host device and, if permitted, for transmitting data from said processor; and

(f) a radio transceiver interface controller for controlling said device radio transceiver.

31. The device of claim 30, wherein said radio transceiver is implemented according

to Bluetooth technology.

32. A system for controlling access to a network resource, the system comprising:

(a) an active data device for controlling access to the network resource, said active data device featuring a device radio transceiver;

(b) a host computational device for communicating with said active data device to provide access to the network resource, said host computational device featuring a radio transceiver for communicating with said device radio transceiver for data exchange with said active data device; and

(c) a network for connecting said host computational device to the network resource.

33. The system of claim 32, wherein said radio transceiver is implemented according to Bluetooth technology.

34. A system for controlling access to stored data, the system comprising:

(a) an electronic data storage device for storing the stored data; and

(b) an access control device for controlling access to said electronic data storage device, such that the stored data is only accessed through said access control device, and such that said access control device determines access to the stored data according to at least one permission.

35. The system of claim 34, wherein said data storage device and said access control device are implemented as a plurality of separate components.

36. The system of claim 34, wherein said access control device further comprises:

(i) an input for receiving a request to access the stored data;

(ii) a non-volatile memory for storing at least one permission for determining access to the stored data;

(iii) at least one instruction for determining a permitted access according to the at least one permission, said at least one instruction being stored on said non-volatile memory; and

(iv) a processor for executing said at least one instruction and for comparing said

request to said at least one permission, such that if said at least one permission includes a type of access requested in said request, the stored data is provided, and alternatively if said at least one permission does not include a type of access requested in said request, the stored data is not provided.

37. The system of claim 36, wherein said non-volatile memory is a flash memory device.

38. The system of claim 37, further comprising:

(c) a CPU (central processing unit) for transmitting said request to said access control device and for receiving provided data; and

(d) a bus for connecting said CPU to said access control device, such that said electronic data storage device is not accessed through said CPU, but only through said access control device.

39. The system of claim 38, wherein said bus is a USB (universal serial bus).

40. The system of claim 39, wherein said at least one permission is for comparing said request to the stored data and for returning a positive or negative comparison, such that if said request is identical to the stored data, said comparison is positive, and alternatively such that if said request is not identical to the stored data, said comparison is negative, and such that the stored data is not read.

41. The system of claim 34, further comprising:

(c) an MP3 player for playing MP3 file data; and

(d) an MP3 interface for said access control device, said MP3 interface enabling said access control device to communicate with said MP3 player to determine access to said MP3 file data.

42. A device for controlling access to data stored in an electronic data storage device, the device comprising:

(a) an input for receiving a request to access the stored data;

(b) a non-volatile memory for storing at least one permission for determining access

to the stored data;

(c) at least one instruction for determining a permitted access according to the at least one permission, said at least one instruction being stored on said non-volatile memory; and

(d) a processor for executing said at least one instruction and for comparing said request to said at least one permission, such that if said at least one permission includes a type of access requested in said request, the stored data is provided, and alternatively if said at least one permission does not include a type of access requested in said request, the stored data is not provided.

43. A method for controlling access to data stored in an electronic data storage device, the method comprising the steps of:

(a) providing an access control device for determining access to the electronic data storage device;

(b) receiving a request to access the stored data by said access control device;

(c) comparing said request to at least one permission for determining access to the stored data by said access control device;

(d) if said at least one permission includes a type of access requested in said request, performing said request for accessing the stored data from the electronic data storage device by said access control device; and

(e) alternatively, if said at least one permission does not include said type of access requested in said request, rejecting said request by said access control device.

44. The method of claim 43, wherein said type of access includes permission to read from the stored data, such that step (d) includes the step of reading from the stored data.

45. The method of claim 44, wherein said type of access includes permission to write to the stored data, such that step (d) includes the step of writing to the stored data.

46. The method of claim 43, wherein said type of access only includes comparing said request to the stored data and for returning a positive or negative comparison, such that if said request is identical to the stored data, step (d) includes the step of returning a positive comparison, and alternatively such that if said request is not identical to the stored data, step (d)

includes the step of returning a negative comparison, such that the stored data is not read.

47. The method of claim 43, wherein the stored data is a credit card number, and said credit card number features a plurality of types of data, each of said plurality of types of data being stored with a separately selected access permission.

48. The method of claim 43, wherein the stored data has a permission for a predetermined number of data read accesses, such that step (c) includes the steps of:

(i) determining a number of performed data read accesses for the stored data; and

(ii) if said number of performed data read accesses is less than said predetermined number of data read accesses, permitting the stored data to be read.

49. The method of claim 43, wherein access is determined for a user and wherein step (b) further comprises the steps of:

(i) collecting a biological parameter of said user; and

(ii) analyzing said biological parameter to determine an identity of said user, such that said at least one permission is determined according to said identity.

50. A device for controlling access to data stored in an electronic data storage device by a user, access being determined according to a biological parameter of the user, the device comprising:

(a) a biometric detection device for detecting said biological parameter of the user and for determining whether the user has said at least one permission to access the stored data;

(b) an input for receiving a request to access the stored data;

(c) a non-volatile memory for storing at least one permission for determining access to the stored data;

(d) at least one instruction for determining a permitted access according to the at least one permission, said at least one instruction being stored on said non-volatile memory; and

(e) a processor for executing said at least one instruction and for comparing said request to said at least one permission, said processor being connected to said biometric detection device, such that if said at least one permission includes a type

of access requested in said request, the stored data is provided, and alternatively if said at least one permission does not include a type of access requested in said request, the stored data is not provided.

ABSTRACT OF THE DISCLOSURE

A device, a method and a system for providing removable, active, personal storage. The device itself features sufficient computational power and resources to perform various tasks with regard to data storage and retrieval. In particular, these resources are provided such that the management of the memory of the storage device is performed at the device level, rather than requiring management by an external operating system, such as the operating system of an external computational device for example. At a minimum, the device features a data processor of some type for executing instructions related to memory management, a flash memory device for storing the data and instructions, a flash controller for controlling access to a flash memory device, a USB controller and a USB connector, for connecting the device to an external computational device through the USB bus of the external computational device.

Figure 1

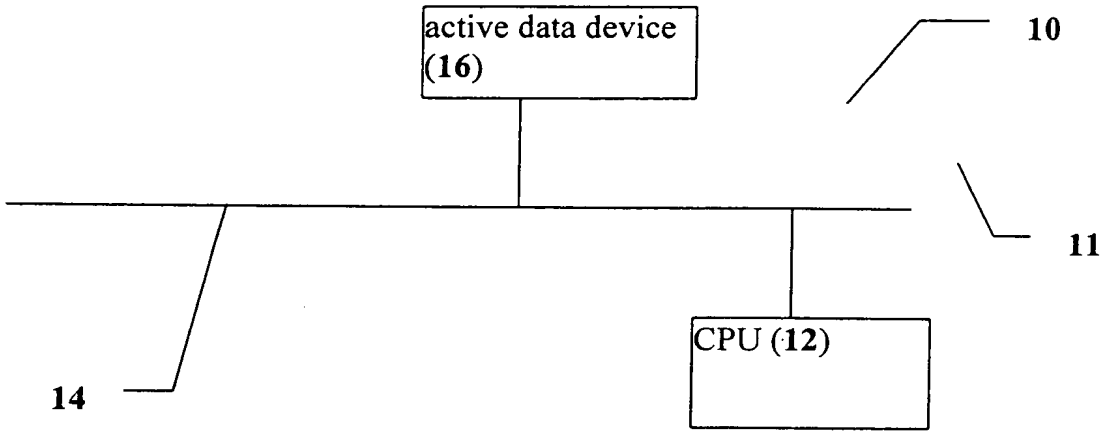


Figure 2

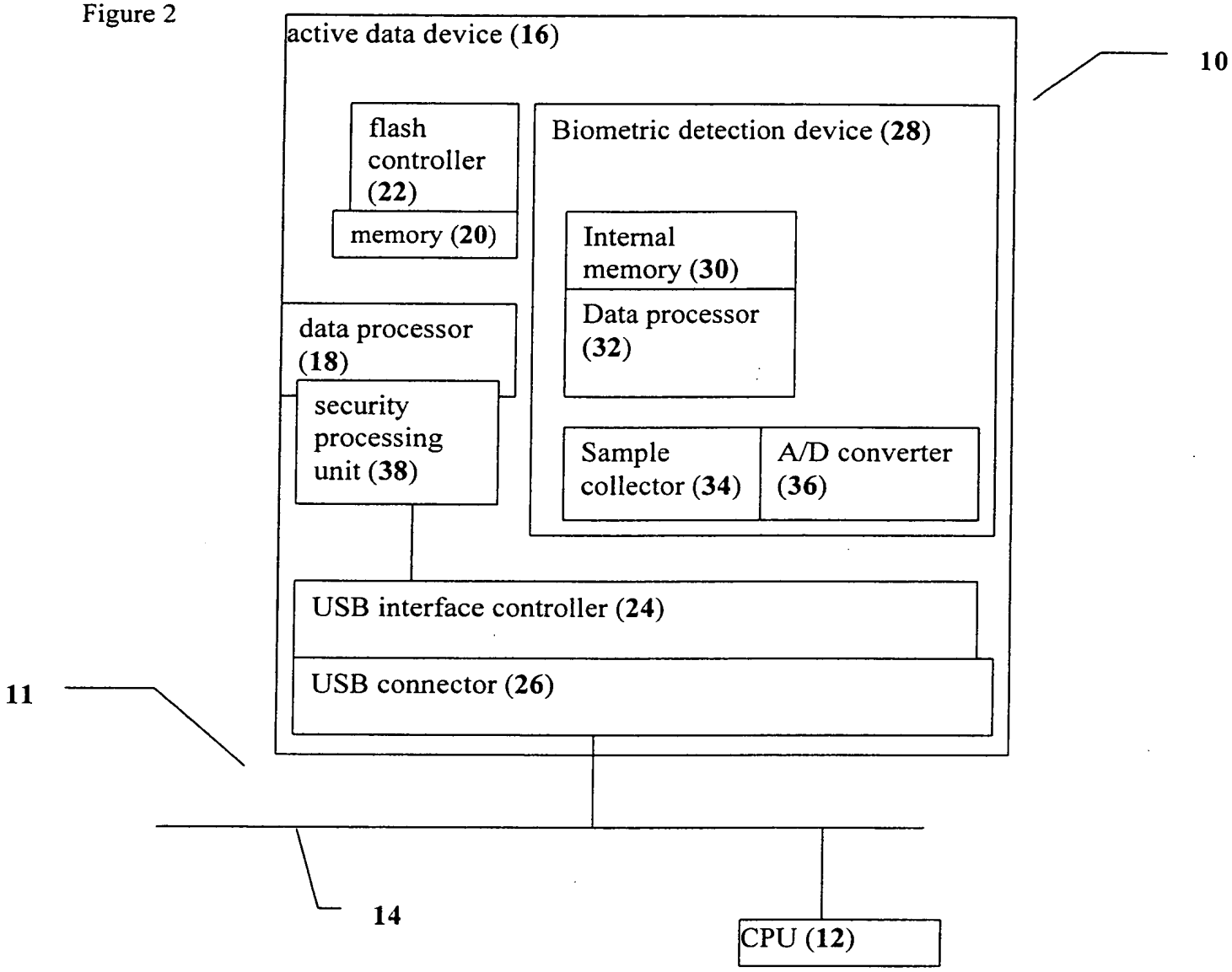

active data device (16)
10
flash controller (22)
memory (20)
Biometric detection device (28)
Internal memory (30)
Data processor (32)
data processor (18)
security processing unit (38)
Sample collector (34)
A/D converter (36)
USB interface controller (24)
USB connector (26)
11
14
CPU (12)

Figure 3

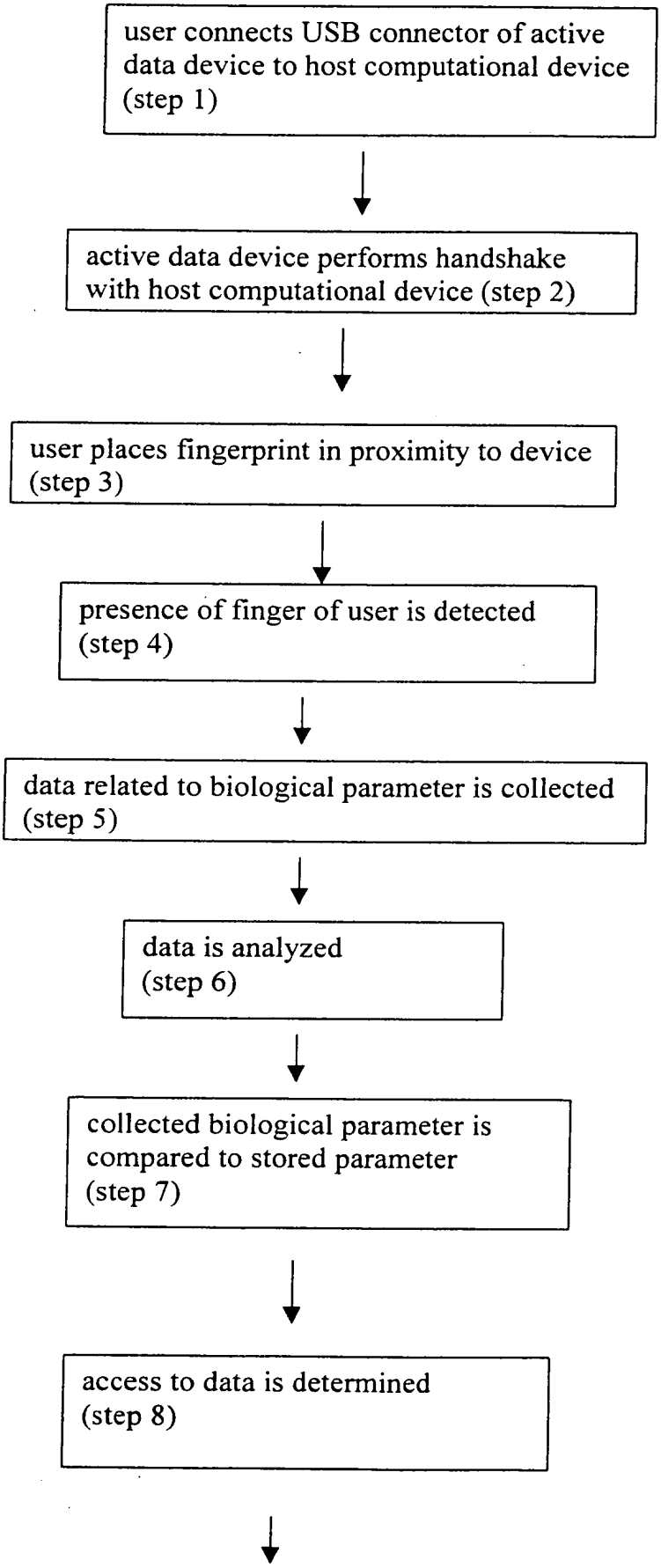

user connects USB connector of active data device to host computational device (step 1)
active data device performs handshake with host computational device (step 2)
user places fingerprint in proximity to device (step 3)
presence of finger of user is detected (step 4)
data related to biological parameter is collected (step 5)
data is analyzed (step 6)
collected biological parameter is compared to stored parameter (step 7)
access to data is determined (step 8)

Figure 3 (con't)

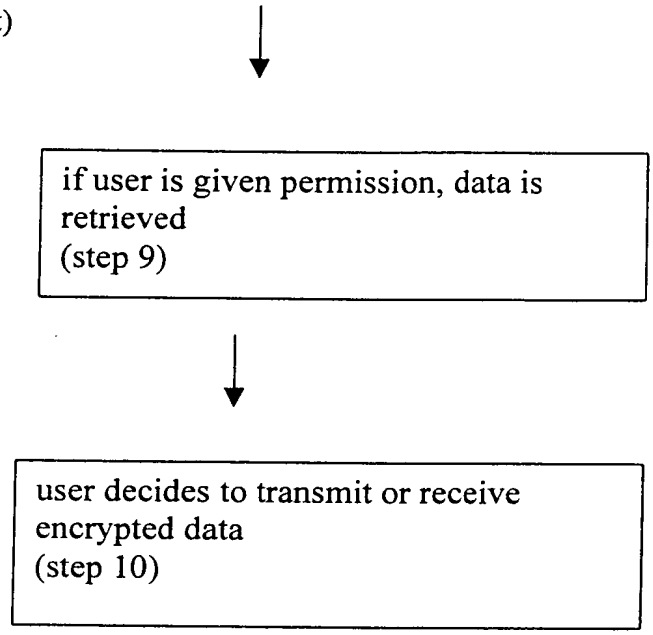


Figure 4

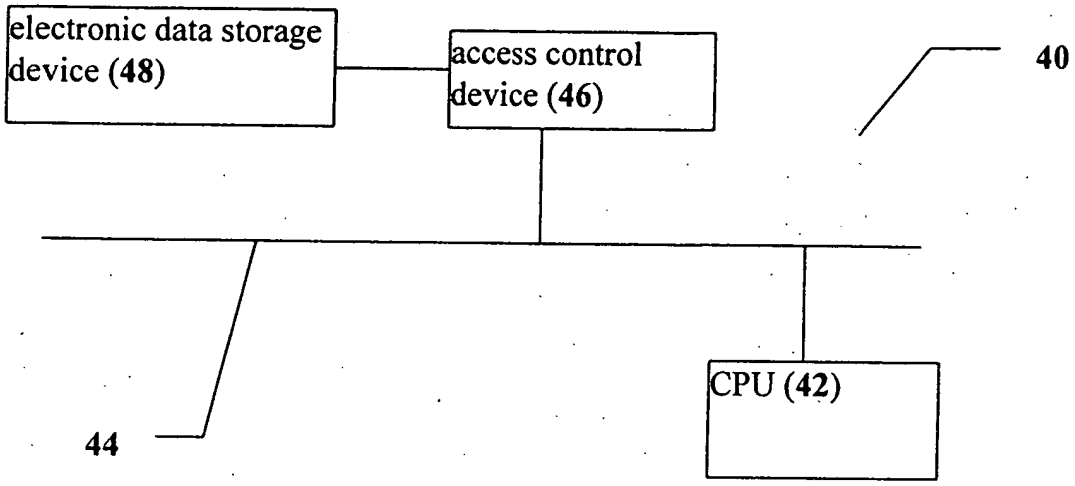
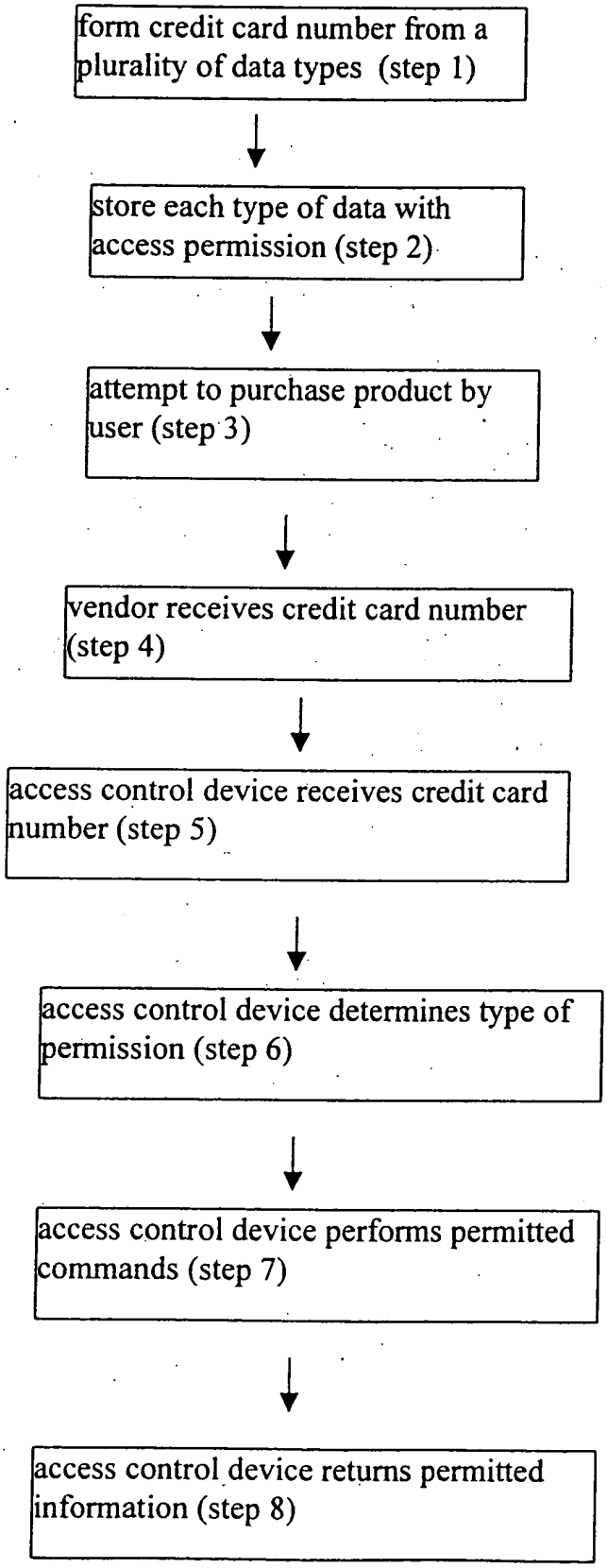

electronic data storage device (48)
access control device (46)
40
CPU (42)
44

Figure 5


form credit card number from a plurality of data types (step 1)
store each type of data with access permission (step 2)
attempt to purchase product by user (step 3)
vendor receives credit card number (step 4)
access control device receives credit card number (step 5)
access control device determines type of permission (step 6)
access control device performs permitted commands (step 7)
access control device returns permitted information (step 8)

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTICE INFORMING THE APPLICANT OF THE COMMUNICATION OF THE INTERNATIONAL APPLICATION TO THE DESIGNATED OFFICES

(PCT Rule 47.1(c), first sentence)

To:
BRASS, Daniel
Plinner, Bodner & Brass
Beit Agish Ravad
13 Noach Mozes Street
67442 Tel Aviv
ISRAËL

Date of mailing (day/month/year) 05 April 2001 (05.04.01)	
Applicant's or agent's file reference M01/3	**IMPORTANT NOTICE**

International application No.	**International filing date** (day/month/year)	**Priority date** (day/month/year)
PCT/IL00/00555	10 September 2000 (10.09.00)	30 September 1999 (30.09.99)

Applicant
M-SYSTEMS FLASH DISK PIONEERS LTD. et al

1. Notice is hereby given that the International Bureau has communicated, as provided in Article 20, the international application to the following designated Offices on the date indicated above as the date of mailing of this Notice:
   AU,KP,KR,US

   In accordance with Rule 47.1(c), third sentence, those Offices will accept the present Notice as conclusive evidence that the communication of the international application has duly taken place on the date of mailing indicated above and no copy of the international application is required to be furnished by the applicant to the designated Office(s).

2. The following designated Offices have waived the requirement for such a communication at this time:
   AE,AL,AM,AP,AT,AZ,BA,BB,BG,BR,BY,CA,CH,CN,CR,CU,CZ,DE,DK,DM,EA,EE,EP,ES,FI,GB,GD,
   GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,
   NO,NZ,OA,PL,PT,RO,RU,SD,SE,SG,SI,SK,SL,TJ,TM,TR,TT,TZ,UA,UG,UZ,VN,YU,ZA,ZW
   The communication will be made to those Offices only upon their request. Furthermore, those Offices do not require the applicant to furnish a copy of the international application (Rule 49.1(a-bis)).

3. Enclosed with this Notice is a copy of the international application as published by the International Bureau on
   05 April 2001 (05.04.01) under No. WO 01/23987

REMINDER REGARDING CHAPTER II (Article 31(2)(a) and Rule 54.2)

If the applicant wishes to postpone entry into the national phase until 30 months (or later in some Offices) from the priority date, **a demand for international preliminary examination** must be filed with the competent International Preliminary Examining Authority before the expiration of 19 months from the priority date.

It is the applicant's sole responsibility to monitor the 19-month time limit.

Note that only an applicant who is a national or resident of a PCT Contracting State which is bound by Chapter II has the right to file a demand for international preliminary examination.

REMINDER REGARDING ENTRY INTO THE NATIONAL PHASE (Article 22 or 39(1))

If the applicant wishes to proceed with the international application in the **national phase**, he must, within 20 months or 30 months, or later in some Offices, perform the acts referred to therein before each designated or elected Office.

For further important information on the time limits and acts to be performed for entering the national phase, see the Annex to Form PCT/IB/301 (Notification of Receipt of Record Copy) and Volume II of the PCT Applicant's Guide.

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No. (41-22) 740.14.35

Authorized officer
J. Zahra

Telephone No. (41-22) 338.83.38